

УНИВЕРЗИТЕТ СИНГИДУНУМ

- МАСТЕР СТУДИЈСКИ ПРОГРАМ -
САВРЕМЕНЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

МАСТЕР РАД

Криптозаштита у комуникационим системима

Ментор:
Проф др Младен Веиновић

Студент:
Југослав Спасојевић
Број индекса: 410177/2012

Univerzitet Singidunum

Београд, 2013.

Криптозаштита у комуникационим системима

Сажетак

У овом раду је описана безбедност и криптозаштита информација у информационо-комуникационим системима. Због чињенице да је решење за заштиту дато кроз слојеве OSI (TCP/IP) модела, наведени су и начини заштите информација за све карактеристичне слојеве. Посебно тежиште рада је дато на безбедносним ризицима којима су изложене информације приликом коришћења мобилних уређаја и решењима за криптозаштиту мобилне телефоније. Такође дате су и неке специфичности криптозаштите информација у радио комуникацијама и значај разумевања појма компромитујуће електромагнетно зрачење и заштите од истог.

Кључне речи: Безбедност информација, безбедносни сервиси и механизми, OSI модел, вишеслојна заштита, шифровање, COMSEC, TRANSEC, KEMЗ.

Abstract

This paper describes the security and cryptographic protection of information in the information and communication systems. Due to the fact that the solution for the protection granted by the layers of the OSI (TCP / IP) model, are listed with their information protection for all characteristic layers. In particular focus is given to the security risks they are exposed to information while using mobile devices and solutions for cryptographic protection of mobile telephony. Also provided are some specifics for the information in radio communications and the importance of understanding the concept of compromising electromagnetic emanation and the protection of the same.

Keywords: Information Security, security services and mechanisms, OSI model, multilayer protection, encryption, COMSEC, TRANSEC, TEMPEST.

САДРЖАЈ

1. УВОД 6
2. МЕТОДОЛОГИЈА ИСТРАЖИВАЧКОГ ПРОЈЕКТА 7
2.1. Уводне напомене и образложење рада 7
2.2. Предмет истраживања 7
2.3. Циљеви и задаци истраживања 7
2.4. Метод истраживања 7
2.5. Истраживачке хипотезе 8
3. ПОЈАМ ИНФОРМАЦИЈА И ЊЕНЕ ОСОБИНЕ 9
3.1. Веродостојност 9
3.2. Правовременост 10
3.3. Актуелност 10
3.4. Поузданост 10
3.5. Релевантност 10
3.6. Потпуност 10
3.7. Непрекидност 10
3.8. Јасноћа 10
3.9. Сажетост 10
3.10. Објективност 10
3.11. Тајност 10
4. БЕЗБЕДНОСТ ИНФОРМАЦИЈА 11
4.1. Нормативна сфера 11
4.2. Организациона сфера 11
4.3. Сфера физичко-техничке заштите 11
4.4. Мере према кадру 11
4.5. Криптолошка сфера заштите 11
5. БЕЗБЕДНОСНИ ТРЕНДОВИ У РАЧУНАРСКИМ СИСТЕМИМА 12
5.1. Друштвене мреже 12
5.2. Додаци за шпијунирање 12
5.3. Сајбер напади 12
6. БЕЗБЕДНОСНИ СЕРВИСИ OSI МОДЕЛА 13
6.1. Безбедносни напади 13
6.1.1. Пасивни напади 14
6.1.2. Активни напади 14
6.2. Безбедносни сервиси 15
6.2.1. Аутентичност 16
6.2.2. Контрола приступа 16
6.2.3. Тајност података 16
6.2.4. Интегритет података 16
6.2.5. Непорецивост 16
6.2.6. Доступност 16
6.3. Примена криптографских техника 16
6.4. Безбедносни механизми 17
7. ВИШЕСЛОЈНА ЗАШТИТА 18
7.1. Заштита на апликативном нивоу 18
7.1.1. S/MIME протокол 19
7.1.2. Kerberos протокол 19
7.1.3. SET протокол 19
7.2. Заштита на транспортном нивоу 19
7.2.1. SSH протокол 19
7.2.2. SSL протокол 19

7.2.3. TLS протокол 20
7.2.4. WTLS протокол 20
7.3. Заштита на мрежном нивоу 20
7.3.1. Firewall 21
7.3.2. IPSec протокол 21
7.4. Заштита на физичком нивоу 22
8. ЕВОЛУЦИЈА ЈАВНИХ МОБИЛНИХ МРЕЖА 22
9. БЕЗБЕДНОСНИ РИЗИЦИ КОРИШЋЕЊА МОБИЛНИХ ТЕЛЕФОНА 24
9.1. Malware и директни напади 24
9.2. Физички напади 24
9.3. Пресретање података, прислушкивање и цурење информација 25
9.3.1. Напади преко Bluetooth интерфејса 25
9.3.2. Напади преко Wireless мреже 25
9.3.3. Прислушкивање 25
9.3.4. „Цурење“ информација 26
9.4. US-CERT препоруке 26
10. ПРИНЦИП ОБРАДЕ ГОВОРНОГ СИГНАЛА 27
11. САВРЕМЕНА РЕШЕЊА ЗА КРИПТОЗАШТИТУ У МОБИЛНОЈ ТЕЛЕФОНИЈИ 28
11.1. Compnautica 28
11.1.1. Концепт решења за заштиту 28
11.1.2. Compumatica SMS 29
11.1.3. Расположиви модели телефона 30
11.1.4. Secure BlackBerry (Compumatica BB) 31
11.2. GSMK 31
11.2.1. Концепт примењене криптозаштите 31
11.2.2. Расположиви модели телефона 31
11.2.3. GSMK CryptoPhone CUG 32
11.3. Casper Technology 33
11.3.1. Cryptech 2G 33
11.3.2. Cryptech Linux 34
11.3.3. Cryptech 3G 34
11.4. Rohde & Schwarz 34
11.4.1. TopSec GSM encrypting mobile phone 35
11.4.2. TopSec Mobile voice encryption device 35
11.4.3. Криптолошки концепт 36
11.4.4. TopSec Mobile за smartphone и laptop 37
11.4.5. Основне карактеристике 37
11.4.6. Криптолошки концепт 37
11.5. Omnisec 38
11.5.1. Основне карактеристике 39
11.5.2. Криптолошке карактеристике 39
12. СПЕЦИФИЧНОСТИ ШИФРОВАЊА ГОВОРА У РАДИО КОМУНИКАЦИЈАМА 40
13. ПОЈАМ КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА 41
14. ЗАКЉУЧАК 42
15. ЛИТЕРАТУРА 43

Слика 1: Пасивни напади 14
Слика 2. Активни напади 15
Слика 3: Примена хибридног криптографског система 17
Слика 4. Веза између безбедносних напада и безбеносних сервиса 18

Слика 5. Компаративни приказ OSI и TCP/IP мрежних модела и предложени систем заштите 18
Слика 6. Успостава конекције између клијентске и серверске стране путем SSL протокола 20
Слика 7. Структура IPSec пакета података за пренос преко Ethernet мрежа 21
Слика 8. IP VPN Encryption HC-7825 10/20/100 Mb/s фирме Crypto AG 21
Слика 9. Уређај за вишегрупну линковску криптозаштиту CD510 22
Слика 10: Основне карактеристике мобилних мрежа 23
Слика 11: Функционални блокови Bluetooth система 25
Слика 12: Шема пасивног напада на мобилни телефон 26
Слика 13: Приступне тачке за безбедносне претње у мобилној телефонији 27
Слика 14: Илустрација комуникационо преносне инфраструктуре 28
Слика 15: Илустрација графичког интерфејса апликације за шифровање SMS 30
Слика 16: GSM QuadBand телефон 30
Слика 17: GMSK CryptoPhone 300 32
Слика 18: GMSK CryptoPhone 301 32
Слика 19: GMSK CryptoPhone 400 32
Слика 20: Key Management Console 33
Слика 21: Cryptech 2G мобилни телефон 33
Слика 22: Криптозаштићена GSM мрежа 33
Слика 23: Cryptech Linux мобилни телефон 34
Слика 24: Илустрација рада у 3G мрежи 34
Слика 25: Криптозаштита у аналогним, дигиталним и мобилним радио мрежама 35
Слика 26: Криптомодул TopSec GSM 35
Слика 27: Уређај TopSec Mobile 36
Слика 28: TopSec Phone апликација 37
Слика 29: TopSec Mobile криптозаштита говора 38
Слика 30: Secure Mobile Phone Omnisec 230 38
Слика 31: Omisec решење за криптозаштиту говора 39

1. УВОД

Примена заштите тајности информација и криптографских сервиса подразумева добро познавање особина информација. OSI (енгл. OSI – Open System Interconnection) референтни модел омогућује систематичан приступ решавања проблема заштите и поуздане механизме за дефинисање безбедносних напада, механизама и сервиса. Безбедносни напади се могу поделити на активне и пасивне, као и групу DOS (енгл. Denial Of Serivce) напада која представља посебну врсту. Безбедносни механизми представљају процесе (или уређаје уграђене као процесе) чија је намена да врше превенцију, детекцију и опорављање након безбедносног напада на систем. На пример, у безбедносне механизме спадају криптографски алгоритми, дигитални потпис, дигитална енвелопа и аутентикациони протоколи. Безбедносни сервиси (у неким књигама познати као криптографски сервиси) обухватају аутентичност, тајност, интегритет, непорецивост, контролу приступа и расположивост. Имајући у виду слојевиту структуру савремених рачунарских мрежа, намеће се идеја да је за реализацију поузданог система заштите неопходно осмислити и применити вишеслојну архитектуру.

Мобилне комуникације нуде бежично повезивање који омогућава мобилност у различитим комуникационим срединама. Велики захтеви тржишта су покретачи развоја мобилних комуникација више и брже него икада пре. Такође, све интезивнији развој технологија је омогућио развој мобилних телекомуникационих мрежа у погледу раста квалитета преноса говорног сигнала, као основног функционалног сервиса, повећања капацитета мобилних мрежа за пренос података и разноврсност сервиса које исте пружају.

Масовност производње је с друге стране омогућио ниже цене и самим тиме већу приступачност мобилних апарата, а самим тиме све масовније коришћење мобилних телефона како у свету тако и код нас. Садашњи мобилни уређаји нису више само телефони, већ представљају мултифункционалне напараве: рачунаре, камере, средста за идентификацију, електронске трансакције ит.д.

Поред коришћења мобилних телефона у грађанству, исти се све више користе као службено комуникационо средство у јавним и безбедносним службама, а због природе информација које се њиме преносе и безбедносних ризика којима су изложене мобилне комуникације, јавља се потреба за додатном заштитом информација у односу на ону која је већ имплементирана у мобилни мрежама. Да би се умањио безбедносни ризик у погледу деконспирисања садржаја и нарушавања квалитета преношеног саобраћаја морамо бити свесни безбедносних претњи којима су учесници у комуникацији, односно мобилни апарати изложени.

Криптозаштита представља један од техничких аспеката заштите информација у комуникационим системима, па ће, поред основних криптографских техника, у овом раду бити изложена нека од решења за криптозаштиту мобилне телефоније која су данас примењена у свету.

У раду су и дате специфичности заштите радио-комуникација кроз дефинисање појмова COMSEC и TRANSEC безбедности. У последњој глави је објашњен појам компромитујућег електромагнетног зрачења и значај заштите од истог.

2. МЕТОДОЛОГИЈА ИСТРАЖИВАЧКОГ ПРОЈЕКТА

2.1. Уводне напомене и образложење рада

Пројектни задатак има за циљ да дефинише појам и особине информација, њихове безбедносне сфере, ризике који угрожавају њихову тајност и интегритет. Такође, сагледавају се потенцијални напади на информационо-комуникационе системе и безбедносни сервиси које треба реализовати кроз примену безбедносних механизама.

Као систематичан приступ решавања заштите информација (података) обрађен је концепт заштите који се заснива вишеслојној заштити базираној на OSI, односно TCP/IP моделу.

Посебно тежише рада представљају, безбедносни ризици у раду са мобилним уређајима и решења за криптозаштиту информација у мобилној телефонији.

Садржај рада се заснива на теоријским и практичним знањима из области криптозаштите информација, као једног од аспеката техничке заштите информација и исуствима из практичне реализације система за заштиту.

2.2. Предмет истраживања

Безбедност информација је стање заштићености информација приликом њиховог примања, обраде, чувања, преноса и коришћења од различитих облика претњи. Она значајно доприноси информационој безбедности која је један од главних аспеката националне безбедности сваке државе.

Значај информационе безбедности условљен је чињеницом да се, паралелно са увођењем информатичко-комуникационих технологија и уопште технолошким развојем, појављују нови ризици и претње у облику могућих напада на доступност, интегритет и поверљивост информација у савременим информационо-комуникационом системима.

Информациона безбедност је предмет општег интересовања, како државних тако и привредних организација. Један од најважнијих задатака је постала разрада и имплементација поузданих метода и средстава заштите информација, тражење системских решења и средстава заштите са применом најефективнијих алгоритама и метода пројектовања средстава заштите информација.

Предмет истраживања је био усмерен на то да се сагледају сви познати начини угрожавања безбедности информација и предложе решења за њихово минимизирање, односно елиминисање кроз познате механизме заштите и примере дате кроз решења за заштиту у мобилној телефонији.

2.3. Циљеви и задаци истраживања

Овај рад је намењен свима који воде рачуна о безбедности информационих система, без обзира да ли се ради о ИКТ менаџерима или техничком особљу, односно инжењерима. Циљ истраживања је био да се онима који користе информационе технологије повећа ниво безбедносне културе и укаже на могуће ризике приликом обраде и преноса информација и предложе решења за њихову заштиту.

2.4. Метод истраживања

Методологија истраживања се свела на коришћење и проучавање јавних извора са Интернета и књига из области заштите информација и имплементације криптографских протокола и систематизацију тако добијених информација.

2.5. Истраживачке хипотезе

Овим радом желе да се докажу следеће хипотезе:

- Информације које се обрађују и преносе путем информационо-комуникационих система су изложене сталним ризицима од компромитације и губитка.
- Подизање укупног нивоа безбедносне културе при коришћењу комуникационих средстава је један од најважнијих аспеката безбедности информација.
- Имплементација безбедносних сервиса кроз примену криптографских техника обезбеђује један од најзначајнијих аспеката техничке заштитте информација.

3. ПОЈАМ ИНФОРМАЦИЈА И ЊЕНЕ ОСОБИНЕ

Сама реч информација (лат. глагол informare) је првобитно била повезана са новинама и обавештењима. Навешћемо неке од савремених дефиниција информација:

„Информација је ресурс данашњице и будућности, али она није попут материје или енергије. Употребом се не троши, расподелом се не смањује. Ако нешто знам могу научити друге, а да сам ништа при томе не губим. Примењујући то што сам сазнао, не само да не губим коришћено знање, већ га оплемењујем праксом.“ - P.Drucker

„Информација (лат. informatio) поучавање, упућивање, упутство, обавештавање, обавештење, распитивање, обавештеност, обавест, извештај, извешће, судско извиђање, истарага.“ Извор: Милан Вујаклија - Лексикон страних речи и израза.

„Информација (лат.), обавештење. У кибернетици означава податак или скуп података на основу којих се управља неком појавом или неким процесом; један од основних појмова кибернетике.“ Извор : Мала енциклопедија Просвета.

Да би уопште говорили о значају заштите тајности информација, као и осталих криптографских сервиса, најпре се морамо упознати са њиховим основним особинама. Најзначајније особине информација[1] су:

- веродостојност (тачност),
- правовременост,
- актуелност,
- поузданост,
- релевантност,
- потпуност,
- непрекидност.
- јасноћа,
- сажетост,
- објективност и
- тајност.

3.1. Веродостојност

Веродостојност или тачност информација је особина без које информација и није права информација, а може да се претвори и у дезинформацију. Тачност информације могли бисмо дефинисати као адекватан израз стварности која је предмет информисања. Међутим, тачност није апсолутни, него релативни израз стварности, тако да се може говорити о већем или мањем степену тачности, односно мањем или већем степену вероватноће и апроксимативности – приближне тачности. На релацији између тих вредности, у пракси је негде допустив већи, а другде мањи степен тачности информација. Већи степен тачности информација бива непосредном подлогом за доношење блиских одлука, одмах изводљивих, с тренутном или краћом важношћу. И обратно, мањи степен тачности допустив је у случајевима збирних (агрегираних) информација које постају подлогом за доношење одлука с дугорочном важношћу, где је у току њихове реализације могућа корекција.

[1] Особине информација и њихове дефиниције (од 3.1. до 3.11.) изворно преузете из референце под редним бројем [1], стране 7-9.

3.2. Правовременост

Актуелна информација је дошла на време кориснику и управо тиме се и актуелизује. Време које је протекло од актуелног догађаја до корисниковог сазнања о њему мора да буде што краће.

3.3. Актуелност

Суштина актуелности јесте у скраћивању времена од догађаја до његовог сазнања, чиме информација добија већи степен важности. С обзиром на то да је живот све динамичнији, промене све брже и разнолике, то је актуелизовање информације све неопходније. То омогућава брже реаговање на све елементе и процесе пословања, па тако и на његову економичност, а кроз то и економичност информација. За актуелност се повезује и благовременост, али није с њоме истоветна, већ је то комплементарна особина информација.

3.4. Поузданост

Поузданост информација у социолошком и техничком смислу, односно спречавање њиховог искривљивања, тражи успостављање одговарајуће контроле информација. У ту сврху у систем се уграђују одређени контролни апарати, било непосредно у самим рачунарима (hardware) или у самим програмима електронске обраде података (software). Организацију информационог система могуће је тако поставити да у себи укључује способност отклањања евентуалних грешака.

3.5. Релевантност

Информација је значајна за корисника и она не садржи непотребне чињенице.

3.6. Потпуност

Све релевантне чињенице садржане су у информацији.

3.7. Непрекидност

Информације треба да пристижу непрекидно и да прате све настале промене стања.

3.8. Јасноћа

Форма информације треба да буде јасна, недвосмислена, разумљива примаоцу.

3.9. Сажетост

Овај захтев је делимично у супротности са захтевом потпуности, али у њиховој равнотежи лежи вештина доброг информисања.

3.10.Објективност

У многим информацијама не дознајемо само стварно стање, него стање какво би пошиљалац желео да буде (или бар одређену деформацију у том правцу), или стање за које пошиљалац претпоставља да ће бити по вољи примаоца. У вези са овим атрибутом проверава се извор информација. Објективност је у директној вези са тачношћу.

3.11.Тајност

Тајност представља захтев да информација буде доступна само овлашћеним лицима. Информација којој није загарантована тајност може проузроковати више штете него користи, јер и пошиљаоца и примаоца може довести у врло тешку ситуацију ако за њих сазна конкуренција, односно противник.

4. БЕЗБЕДНОСТ ИНФОРМАЦИЈА

Сам значај информације захтева механизме како би се постигла безбедност информација, било да се ради о резидентним информацијам или пак о информацијама у самом поступку њихове размене у међусобној комуниикацији две стране. Безбедност информација може се поделити на више безбедносних сфера. У поменуте сфере спадају:

- нормативна сфера,
- организациона сфера,
- сфера физичко-техничке заштите,
- мере према кадру и
- криптолошка сфера заштите.

4.1. Нормативна сфера

Нормативна сфера обезбеђује права и обавеза субјекта у одређеним околностима што је регулисано одговарајућим нормативима и актима. Нормативи обавезују и прописују извршење неке радње и начин извршења те радње, као и одговарајуће санкције приликом кршења прописаних права.

4.2. Организациона сфера

Ако посматрамо једну организацију све организационе целине су надлежне за заштиту информација. Надлежности, права и обавезе, организационих целина па и појединаца дефинишу се планом заштите и систематизацијом у којој се прописују и права и обавезе у вези са заштитом за свако појединачно радно место. Свака организациона целина треба да има свој реферат за безбедност и свог локалног референта за безбедност коме су нормативним актима прописане основне дужности о обавезе. Овај субјекат интегрише све сфере безбедности на свом нивоу. Из тог разлога можемо рећи да се организациона сфера заштите информација налази на самом врху хијерархијског прегледа сфера заштите и да она обухвата све остале сфере.

4.3. Сфера физичко-техничке заштите

Ова сфера подразумева мере које се реализују већ од почетка рада на грађевинском пројекту. Грађевински пројекат мора да води рачуна о локацији дате организационе целине, на пример у односу на: спрат, страну света у објекту где је лоцирана, положају у односу на далеководе, гасоводе, емисију штетних гасова из фабрика, све врсте инсталација у згради: водоводне, електричне и гасоводне. Локација организационе целине детерминише заштиту решеткама, бравама, системом видео надзора, алармним системима, пријавном – чуварском службом итд. Сфера физичко-техничких мера подразумева и употребу техничких средстава почевши од сигуроносних брава на уласку у просторију, разних облика закључавања и заштите радних станица (рачунара, терминала), проверу идентификације корисника по принципу: **оно што јесу, оно што знају, оно што имају и како се понашају.**

4.4. Мере према кадру

Напади на било који безбедносно осетљив организациони систем не почињу сами од себе, њих започиње човек, отуда у први план стављамо човека као главни фактор безбедности једног оваквог система. Решење проблема кадровске политике може да се сведе на правилан избор (селекцију) кадрова и обезбеђење оптималних радних услова.

4.5. Криптолошка сфера заштите

Ова сфера обухвата скуп мера и поступака који се примењују у циљу заштите тајних информација од интереса за одређени систем при њиховом преносу телекомуникационим

средствима или складиштењу, односно чувању. Своја достигнућа, мере и поступке које обухвата темељи на достигнућима математике и криштологије.

5. БЕЗБЕДНОСНИ ТРЕНДОВИ У РАЧУНАРСКИМ СИСТЕМИМА

Са увођењем рачунара у интензивну употребу, евидентно је да се јавља потреба за развојем аутоматизованих алата за заштиту фајлова али и других информација које се складиште у самом рачунару. То је посебно значајно за тзв. дељене системе (ресурсе), а далеко је значајније за системе којима се приступа преко јавне телефонске мреже, мреже за пренос података или преко Интернета. Један од најпопуларнијх типова напада на информационе системе је рачунарски вирус. У рачунарски систем вирус може да доспе физички преко неког од физичких медиума за пренос података (дискета, оптички диск, USB flash) или преко Интернета. У било ком случају, када је рачунар једном заражен вирусом, неопходно је постојење рачунарских програма и алата за заштиту и опоравак од последица напада вируса.

5.1. Друштвене мреже[2]

Друштвене мреже (social networks) су трансформисале Интернет у моћан комуникациони медијум и привукле милионе корсника, али и отвориле нове опасности по њихову приватност и безбедност. Ово је изражениje у друштвеним мрежама опште намене (као што је Facebook, Twitter или MySpace) и ако се корисник укључује с мобилног терминала. Повреде приватности и угрожавање безбедности могу потицати и од других учесника у друштвеној мрежи, трећих лица и самог пружаоца услуге друштвене мреже, а најчешће су крађа идентитета, злоупотреба или фалсификовање података, одлив пословних информација и угрожавање репутације предузећа, лоцирање и праћење корисника, социјални инжењеринг, лажно представљање. Поред набројаних ризика, друштвене мреже су идеалан канал за ширење злоћудних програма.

5.2. Додаци за шпијунирање

Програмски додаци за шпијунирање (spyware) су апликације које се инсталирају на персонални рачунар или мобилни телефон, и без видљивих знакова прикупљају и шаљу информације о комуникацијама и другим активностима корисника. Ова врста злоћудног софтвера одавно се раширила на Интернету, а последњих година, са развојем и публиковањем архитектура и отварањем програмских интерфејса, озбиљно угрожава и мобилне уређаје. Потенцијални корисници шпијунског софтвера могу бити забринути родитељи, љубоморни супружници или партнери, сумњичави послодавци, индустријски шпијуни, криминалци и многи други. На данашњем нивоу развоја мобилни spyware подржава тајну крађу информација са уређаја, слање SMS и MMS на рачун жртве, лоцирање у реалном времену, укључивање микрофона и прислушкивање простора, пресретање свих (говорних и неговорних) комуникација. Прогнозе су суморне, нарочито за мобилни spyware: напади су неизбежни и биће све комплекснији и вирулентнији, све више ће погађати корпоративни сектор и сектор електронског пословања, корисници ће све теже моћи да се одбране од њих, тако да ова претња, по свим скорашњим проценама, улази међу првих 10 претњи по безбедност информација у електронским комуникацијама.

5.3. Сајбер напади

Организовани сајбер криминал препознат је као посебно озбиљна претња по безбедност информација и електронских комуникационих мрежа. Сведоци смо настајања глобалне подземне економије која, иако криминална, функционише по свим законитостима легалне економије: има препознатљив пословни модел који обухвата намеру, средства, план, циљну групу, поделу улога, инфраструктуру, механизме извлачења добити, послује на

[2] Текст из тачака 5.1., 5.2, 5.3. изворно преузет из референце под редним бројем [4].

принципима понуде, тражње и репутације „привредника“ на бази потврђених успеха, али увек са примарним циљем: доћи до новца и не бити ухваћен.

Сајбер тероризам, сајбер рат и безбедност критичне инфраструктуре постају нови, све значајнији елементи војно-политичких доктрина многих земаља. Од једноставних експеримената чији циљ је био самодоказивање аутора, сајбер напади су прерасли у комплексне операције које се изводе ради профита или из политичких разлога. Напад у сајбер простору је јефтин, порецив и лако се прикрива. С друге стране, може да нанесе огромну штету жртвама. Танка линија раздвајања сајбер криминала, сајбер тероризма и рата у сајбер простору данас је потпуно избледела; има индиција да неке земље виде криминалне и терористичке групе као корисне савезнике и да су већ показале спремност да толеришу, охрабрују, па чак и усмеравају појединце и групе да нападају непријатељске циљеве. Све већа зависност националних економија и државне управе од критичне информационо-комуникационе инфраструктуре, њена узајамна и прекогранична повезаност са другим инфраструктурама, у окружењу бројних претњи и ризика, као императив намећу потребу за систематским решавањем проблема супротстављања сајбер нападима великих размера.

6. БЕЗБЕДНОСНИ СЕРВИСИ OSI МОДЕЛА

Препорука X.800 (Security Architecture for Open Systems Interconnection) представља препоруку која проблеме безбедности дефинише на један систематичан начин. Ово је препоруку је развио сектор за стандардизацију у области телекомуникцаија међународне телекомуникационе уније (ITU-T).

OSI архитектура безбедности је поуздан начин за организацију задатака за решавање безбедносних проблема и задовољавање безбедносних захтева. Ова архитектура се фокусира на **безбедносне нападе, механизме и сервисе**.

Препоруком X.800 се укратко дефинишу дати појмови на следећи начин:

- Безбедносни напад – било која акција која компромитује информације које припадају некој организацији;
- Безбедносни механизам – било који процес (или уређај који је уграђен као један процес) који је дизајниран да врши превенцију-спречавање потенцијалних напада, да детектује потенцијалне нападе и да омогући опоравак од потенцијалних напада;
- Безбедносни сервиси – сервиси обрађивања података или комуникациони сервиси који повећавају безбедност система у току обраде података, као и у току преноса података путем комуникационих канала. Дати сервиси су намењени да одбијају безбедносне нападе, и они могу да користе један или више безбедносних механизама да би обезбедили дате сервисе.

6.1. Безбедносни напади

Безбедносни напади се могу поделити на **пасивне и активне**. Пасивни напади покушавају да истраже систем или користе информације које се преносе истим, али при томе не користе његове ресурсе.

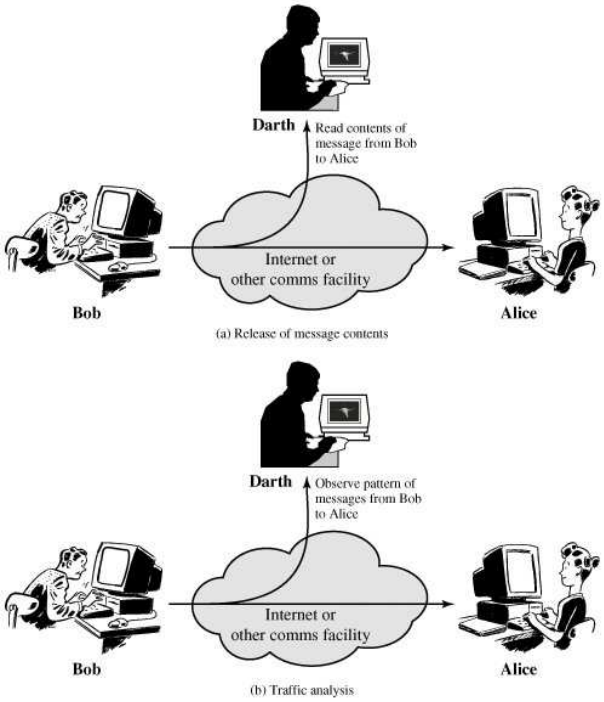
Ативни напади покушавају да измене системске ресурсе (укључујући и информације које се преносе системом) или да измене операције самог система.

6.1.1. Пасивни напади

Пасивни напади су познати као прислушкивање, односно надгледање преносних канала. Њихов циљ је да открију садржај порука које се преносе комуникационим каналом.

Постоје два типа пасивних напада: откривање информационог садржаја поруке и анализа саобраћаја (слика 1.).

Док је први тип напада сам по себи разумљив, други подразумева анализу маскираног, односно шифрованог, саобраћаја како би се рецимо одредила локација и идентитет учесника у комуникацији, као и дужина и учесталост порука које се преносе путем комуникационог канала.



Слика 1: Пасивни напади

6.1.2. Активни напади

Активни напади проузрокују одређене модификације токова података као и креирање лажних токова података. Могу да се поделе на следеће типове: лажно представљање, понављање слања послатих порука, генерисање лажних или модификација легалних порука и неауторизивано коришћење рачунарских ресурса.

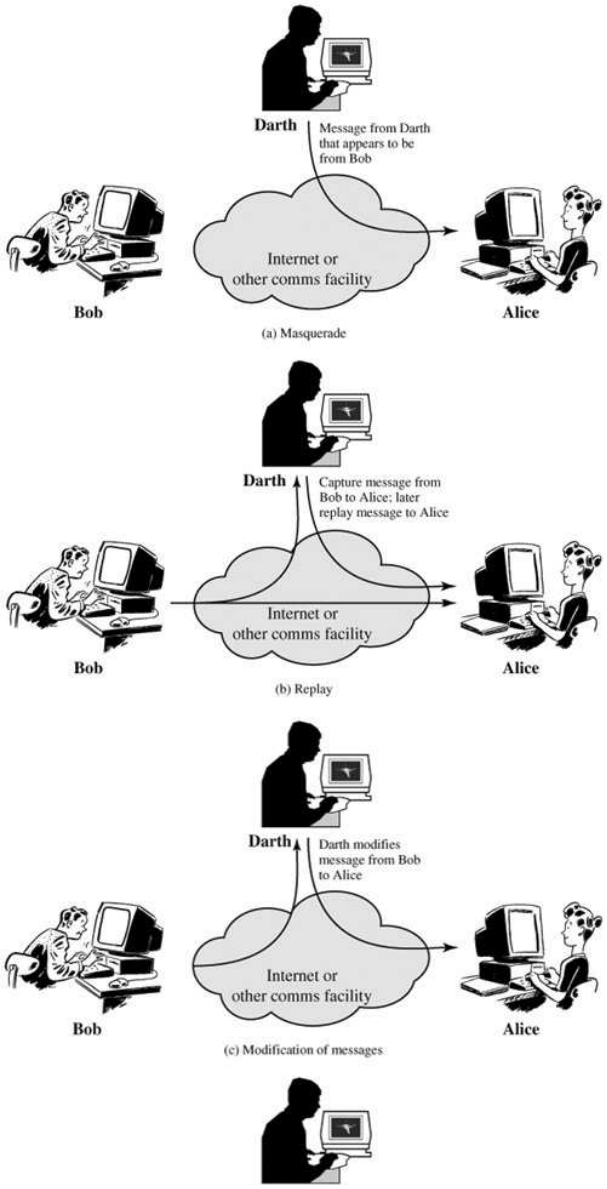
Лажно представљање (енгл. masquerading) је врста напада у којој нападач покушава да искористи туђи идентитет ради напада на рачунарски систем.

Понављањем слања послатих порука, иако су оне рецимо шифроване, неовлашћени корисник може угрозити оптеретити систем, односно угрозити његову функционалност

Генерисање лажних или нелегална модификација порука, које се преноси у дистрибуираном окружењу, један је од напада који могу да нанесу највише штете легалним учесницима у комуникацији, јер се тиме нарушава интегритет порука, односно саобраћаја.

Неауторизовано коришћење рачунарских ресурса најчешће се испољава кроз напад типа укидање сервиса (Denial of Service - DoS). Основни циљ те врсте напада јесте нарушавање исправног рада расположивих сервисних програма у систему.

Илустрација активних напада је дата на слици 2.



Слика 2. Активни напади

6.2. Безбедносни сервиси

Безбедносни сервиси представљају сервисе обрађивања података или комуникационе сервисе којима систем обезбеђује специфичну врсту заштите својим ресурсима и имплементирани су кроз безбедносне механизме. X.800 дефинише безебедоносне сервисе као сервисе реализоване путем протокола на различитим нивоима OSI архитектуре, који обезбеђују безбедност система или информација које се преносе. Постоји пет категорија безбедносних сервиса:

- аутентичност,
- контрола приступа,
- тајност података,
- интегритет података,
- непорецивост и
- доступност.

6.2.1. Аутентичност

Сервис аутентичности обезбеђује да стране у комуникацији могу међусобно да утврде идентитет, како при успостави везе тако и током преноса података, али тако да се онемогући присуство неауторизоване особе. Пример за овај сервис је online банкарска трансакција при којој и корисник и банка требају да буду уверени у идентитет друге стране.

6.2.2. Контрола приступа

Контрола приступа представља способност да се ограничи или контролише приступ, преко комуникационог линка, host рачунарима и апликацијама које се на њима извршавају. Да би се то постигло, сваки ентитет најпре мора да се идентификује или да се оствари увид у његову аутентичност. Кориснику банкарског рачуна је дозвољено да види стање на свом рачуну, али не и нечији други.

6.2.3. Тајност података

Тајност података представља сервис којим се постиже заштита података, који се преносе, од пасивних напада. Другим речима, овај сервис задовољава захтев да информациони садржај криптографски заштићене поруке буде доступан само овлашћеним лицима. Овим сервисом се постиже заштита тајности свих података који се размењују између два или више ентитета.

6.2.4. Интегритет података

Интегритет података може бити примењен на ток прука, на појединачну поруку, или на одабрана поља у оквиру поруке. Међутим, најкориснија и најпотпунија заштита је она која штити цео ток података. Овај сервис представља заштиту од активних напада, као што су: брисање, модификација, убацивање или понављање података.

6.2.5. Непорецивост

Непорецивост (енг. non-repudiation) је сервис којим се спречава могућност порицања реализације одређених активности корисника који учествују у комуникацији.

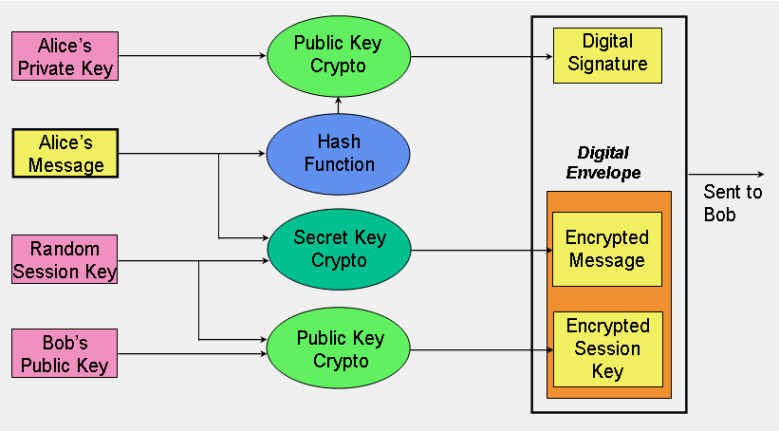
6.2.6. Доступност

Овај сервис обезбеђује доступност систему, на пример представља одбрану од DoS напада и зависи од других безбедносних сервиса као што су контрола приступа, аутентикација ит.д.

6.3. Примена криптографских техника

У остварењу безбедносних захтева у комуникационим системима примењују се технике симетричне или тајне и асиметричне или криптографије јавног кључа. Криптографски системи који комбинују наведене криптографске технике називај се хибридни криптографски системи.

Слика 3. илуструје примену хибридног криптографског система, који се састоји од дигиталног потписа и дигиталне анвелопе (дигитални коверат), у остварењу безбедносних захтева (поверљивост, интегритет, аутентичност и непорецивост) приликом слања и пријема поруке. У овом примеру, пошиљалац поруке је Алиса, а примаоц поруке је Боб.



Слика 3: Примена хибридног криптографског система

Дигитална коверта садржи шифровану поруку и шифровани сесијски кључ. Алиса користи симетрични криптографски алгоритам ради шифровања поруке користећи сесијски кључ, који се генерише случајно. Алиса затим шифрује сесијски кључ помоћу Бобовог јавног кључа. Шифрована порука и шифровани сесијски кључ заједно чине дигиталну анвелопу. Након пријема, Боб дешифрује сесијски кључ користећи свој приватни кључ, а затим дешифрује шифровану поруку.

Дигитални потпис се формира у два корака. Прво, Алиса израчунава хеш вредност њене поруке, а затим шифрује хеш вредност са својим приватним кључем. Након пријема дигиталног потписа, Боб добија хеш вредност коју је израчунала Алиса тако што дешифрује дигитални потпис Алисиним јавним кључем. Боб онда примењује хеш функцију на оригиналној Алисиној коју је претходно дешифровао. Ако резултантна хеш вредност није иста као вредност коју је добио од Алисе, онда Боб зна да је порука измењена, а ако су хеш вредности исте, Боб тада верује да је порука коју је добио идентична са оном коју је послала Алиса.

6.4. Безбедносни механизми

Применом безбедносних механизама врши се имплементација основних безбедносних сервиса. На слици 4. је дата веза између безбедносних сервиса и напада. Безбедносни механизми се деле а две групе: механизми које је могуће имплементирати протоколом на неком од нивоа OSI архитектуре и они механизми који нису специфични за било који специфични проторкол на неком од OSI нивоа. Према X.800, у специфичне безбедносне механизме спадају: шифровање, дигитални потпис, дигитална анвелопа, механизми контроле приступа, аутентикациони протоколи итд.

Security Dimension	X.800 Security Threats				
	Destruction	**Corruption**	**Removal**	**Disclosure**	**Interruption**
Access Control	✓	✓	✓	✓	
Authentication			✓	✓	
Non-Repudiation	✓	✓	✓	✓	✓
Data Confidentiality			✓	✓	
Communication Security			✓	✓	

Data Integrity	✓	✓			
Availability	✓				✓
Privacy				✓	

Слика 4. Веза између безбедносних напада и безбеносних сервиса

7. ВИШЕСЛОЈНА ЗАШТИТА

Имајући у виду слојевиту структуру савремених рачунарских мрежа, намеће се идеја да је за реализацију поузданог система заштите неопходно осмислити и применити вишеслојну архитектуру. На слици 5. приказан је компаративни приказ OSI и TCP/IP мрежних модела и предложени системи заштите. Увођењем додатних заштитних слојева повећава се укупна безбедност система. Па према томе имамо заштиту на: апликативном, транспортном, мрежном и физичком слоју OSI модела.

<table>
<tr><th>OSI #</th><th>OSI
Layer Name</th><th>TCP/ IP #</th><th>TCP/IP
Layer Name</th><th>Security</th></tr>
<tr><td>7</td><td>Application</td><td rowspan="3">4</td><td rowspan="3">Application</td><td>Application</td></tr>
<tr><td>6</td><td>Presentation</td><td rowspan="2">End-to-end
Security</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td rowspan="2">4</td><td rowspan="2">Transport</td><td rowspan="2">3</td><td rowspan="2">Transport</td><td>Transport</td></tr>
<tr><td>Transport Layer
Security</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Network</td><td rowspan="2">2</td><td rowspan="2">IP</td><td>IP</td></tr>
<tr><td>IP Security</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Data Link (LLC
& MAC)</td><td rowspan="3">1</td><td rowspan="3">Network
(interface)</td><td>Network
(interface)</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2">Physical</td><td rowspan="2">Link/Physical
Security</td></tr>
</table>

Слика 5. Компаративни приказ OSI и TCP/IP мрежних модела и предложени систем заштите

7.1. Заштита на апликативном нивоу

Заштита на апликативном нивоу („са краја на крај“, енг. „end-to-end“) се заснива на примени технологије дигиталног потписа на бази асиметричних криптографских алгоритама и заштите тајности података применом симетричних криптографских алгоритама. Применом овог нивоа заштите обезбеђује се: провера аутентичности корисника сервиса мреже како у процесу успостављања комуникације (end-user authentication), тако и у процесу контроле приступа (access control) ресурсима мреже, заштита интегритета података, заштита од могућности накнадног порицања о слању порука, као и заштита тајности података.

Најпознатији протоколи заштите на апликативном нивоу који се примењују у мрежама Интернет/Интранет типа су: S/MIME (енгл. S/MIME – Secure Multipart Internet Mail Extensions), Kerberos, SET (енгл. SET – Secure Electronic Transactions) и други. Ти системи се базирају на примени асиметричних и симетричних криптографских алгоритама и дигиталним сертификатима, као једнозначним параметрима идентификације страна у комуникацији. У савременој криптографији за заштиту електронске поште се, уместо PGP (енгл. PGP – Pretty Good Privacy) протокола, чешће користи S/MIME протокол.

7.1.1. S/MIME протокол

S/MIME је протокол за шифровање и дигитално потписивање мејлова у MIME формату. Овај протокол се заснива на употреби сертификата које издају специјализоване компаније као VeriSign, Thavte или Comodo Group. Сваки сертификат садржи два кључа: јавни и тајни. Они се користе различито, у зависности да ли пошиљалац жели да шифрује или потпише поруку.

7.1.2. Kerberos протокол

Kerberos је протокол који на бази симетричних криптографских алгоритама, посредством активне треће стране од поверења, реализује размену сесијских кључева и аутентикацију учесника у комуникацији.

7.1.3. SET протокол

Secure Electronic Transaction (SET) је протокол, развијен касних 90-тих година за потребе Visa и MasterCard, је намењен за мрежне трансакције преко Интернета у којима се користе платне картице. Овим протоколом се обезбеђује тајност информација, интегритет инструкција за плаћање роба и аутентификацију, како власника картице и тако и трговца.

7.2. Заштита на транспортном нивоу

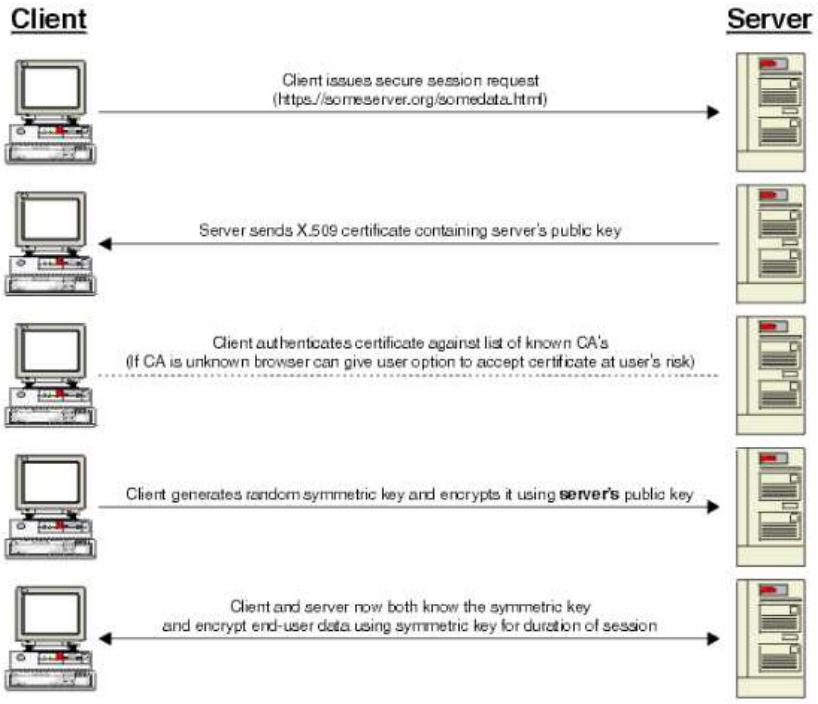
Овај вид заштите представља заштиту тајности података применом симетричних криптографских алгоритама и узајамне провере идентитета субјеката комуникације. Овај ниво штити комуникацију субјеката од интерних и екстерних напада применом криптографских тунела (заштићених сесија) између чворова комуникационог сегмента мреже на бази симетричних криптографских система и применом процедуре „јаке“ аутентикације (strong authentication) између субјеката комуникације. Додатном применом симетричних криптографских система на транспортном нивоу реализују се функције заштите интегритета података који се преносе кроз мрежу и немогућност порицања емисије датих података. Најпознатији коришћени протоколи су: SSH (енгл. SSH – Secure Shell), SSL (енгл. SSL – Secure Sockets Layer), TLS (енгл. TLS – Transport Layer Security) и WTLS (енгл. WTLS – Wireless Transport Layer Security).

7.2.1. SSH протокол

Протокол SSH се најчешће користи за реализацију безбедног удаљеног приступа рачунару (remote login), извршења команди на датом рачунару и копирање датотека између рачунара који комуницирају.

7.2.2. SSL протокол

Најчешће коришћени протокол је SSL (слика 6.) и састоји се из две фазе: аутентикације која се базира на примени асиметричних криптографских алгоритама и размени дигиталних сертификата, у којој се проверава аутентичност страна у комуникацији и размена сесијског кључа, и криптографског тунела који се базира на примени симетричног алгоритма са сесијским кључем који је пренесен у фази аутентикације.



Слика 6. Успостава конекције између клијентске и серверске стране путем SSL протокола

7.2.3. TLS протокол

TLS протокол представља у ствари напреднију везију SSL протокола (на сталу од верзије SSL 3.0). Главна разлика између SSL и TLS је у томе што, док SSL везу почиње након успоставе сигурног канала, TLS конекција ће прво почети са несигурним „hello“ на серверу и тек након успешног „handshake“ процеса између клијента сервера „пребацује се“ на сигурну комуникацију. Ако TLS handshake не успе из било ког разлога, веза се не успоставља.

7.2.4. WTLS протокол

Протокол WTLS је бежична варијанта SSL протокола и служи за заштиту на транспортном нивоу између WAP (енгл. WAP – Wireless Application Protocol) мобилних телефона и WAP сервера на истим принципима (аутентикација и криптографски тунел), као и SSL протокол.

7.3. Заштита на мрежном нивоу

Заштита на мрежном нивоу обезбеђује заштиту између мрежних чворова и штити читав дистрибуирани рачунарски систем од спољашњих напада коришћењем:

- заштитних механизама које пружа стандардна комуникациона опрема
- поступака заштите применом мрежних баријера (firewall)
- заштитних механизама на мрежном нивоу које пружа оперативни систем
- физичких мера заштите приступа рутерима и серверима и
- примена криптографских техника и протокола.

На мрежном нивоу врши се заштита интегритета, тајности и аутентикација IP пакета. Заштита интегритета и аутентикација IP пакета најчешће се реализује применом криптографских компресионих функција са употребом тајног кључа (енгл. MAC – Message Authentication Code), док се заштита тајности остварује применом симетричних алгоритама. Најпознатији протокол заштите на мрежном нивоу јесте IPSec протокол (енгл. IPSec – Internet Protocol Security).

7.3.1. Firewall

Firewall прати сав саобраћај кроз мрежу и штити мрежу од упада неауторизованих корисника. Најчешће коришћени типови филтрирања применом firewall-а су:

- у зависности од IP адреса - омогућава забрану конекција од или према одређеним рачунарима и/или мрежама, у зависности од нихових IP адреса и
- у зависности од портова омогућава забрану конекција од или према одређеним рачунарима и/или мрежама, у зависности од броја порта.

7.3.2. IPSec протокол

IPSec протокол је настао је као резултат иницијативе да се развије јединствени сигурносни механизам за заштићени пренос података у IP мрежама. Развијен је од Internet Engineering Task Force (IETF) групе и представља проширење основног IP протокола. IPSec протокол је саставни део мрежног слоја. IPSec протокол задржава компатибилност с постојећим IP протоколом и омогућава мрежној опреми заснованој на IP протоколу транспарентност у односу на IPSec протокол. Само два крајња учесника у комуникацији, пошиљалац и прималац, морају имати подршку за комуникацију IPSec протоколом. Мрежа чворишта и рутера између крајњих учесника, због компатибилности IPSec протокола с IP протоколом, не мора бити опремљена програмском подршком за IPSec протокол.

Структура IPSec пакета података за комуникацију у Ethernet мрежама приказана је сликом 7. Поље са IPSec заглављем и подацима укључује TCP заглавље, као и сва остала заглавља и податке виших слојева у шифрованом облику.

Ethernet заглавље	IP заглавље	IPSec заглавља и подаци	Ethernet заштита

Слика 7. Структура IPSec пакета података за пренос преко Ethernet мрежа

IPSec протокол омогућава стварање структре сигурне виртуалне приватне мреже (енгл. VPN – Virtual Private Network) изграђене на инфраструктури постојеће јавне IP мреже, односно Интернета, у којој нису задовољени захтеви у погледу сигурности комуникације.

IPSec се базира на асиметричним криптографским системима (углавном) за реализацију аутентикације и симетричним системима за шифровање IP пакета. Постоје различите варијанте овог протокола а најбезбедније су оне које користе шифровање читавих IP пакета (заједно са хедером и IP адресама) обезбеђујући на тај начин да се из спољњег света види само адреса појединих IPSec сервера (VPN гејтвеја), али не и рачунара који у ствари комуницирају.

На слици 8. је приказано хардверско решење швајцарске фирме Crypto AG за IPSec VPN комуникацију удаљених LAN мрежа кроз несигурну WAN структуру, које користи сопствено криптолошки алгоритам (HCA-480, алгоритам произвођача) за шифровање.



Слика 8. IP VPN Encryption HC-7825 10/20/100 Mb/s фирме Crypto AG

7.4. Заштита на физичком нивоу

Физички слој дефинише сам кабал или физички медијум, односно електричне и физичке карактеристике интерфејса уређаја који се прикључују на комуникациону инфраструктуру. Заштита података на овом слоју се своди на заштиту на нивоу електричних импулса, односно бита и користи се за такозвано „шифровање по правцу“ (енгл. link encryption). Баш због тога што се шифрује целокупан саобраћај само између два комуникациона чворишта, овај тип заштите је најбезбеднији, јер није могуће утврдити поред садржаја порука ни идентитет учесника у комуникацији.

Најпознатији комуникациони протоколи за пренос података су Fast Ethernet, RS232, ATM, G.704 уз коришћење електрично-физичких интерфејса типа EUROCOM, G.703 и V11. Криптозаштита на физичком нивоу је карактеристична за стационарне системе преноса капацитета 155/622Mb/s (STM1/STM4) и већим и мобилне тактичко комуникационе системе и једно такво решење је норвешке фирме Kongsberg приказано на слици 9.



Слика 9. Уређај за вишегрупну линковску криптозаштиту CD510

CD510 је уређај криптозаштите који може да штити 5 независних линкова (multi-bulk encryption) на брзинама од 256 / 512 / 1024 / 2048 / 8448 (V11) kb/s при чему врши аутоматску адаптацију на брзину преноса података комуникационог система. Сесијски кључ за шифровање се генерише на бази мастер комуникационих кључева и мења се приликом сваке нове успоставе комуникационог линка.

8. ЕВОЛУЦИЈА ЈАВНИХ МОБИЛНИХ МРЕЖА

Радио-мобилне мреже се развијају од средине двадесетих година прошлог века и то углавном у полицијске и војне сврхе. Комерцијална, односно масовна, примена мобилне телефоније, какву ми сада знамо, почела је са открићем ћелијског (целуларног) система мобилне телефоније.

Прве аналогне целуларне мреже (1G) комерцијално су уведене у САД 1978. године и заснивале су се на AMPS (Advanced Mobile Phone System) систему и од сервиса су имале само говорну комуникацију.

Specifications	Protocol	Maximum Speed	Features
1G analog networks	AMPS	N/A	• Voice service only (analog) • No data service
	DataTAC		
	FDMA		
	Mobitex		
	NMT		
	TACS		
2G	CDMA	Up to 20Kbps	• Digital voice service • Push-to-Talk (PTT) • Short Message Service (SMS) • Conference calling • Caller ID • Voice mail • Simple data applications such as email and Web browsing
	GSM		
	iDEN		
	PCS		
	TDMA		
2.5G	CDMA2000 1xRTT	Up to 144Kbps (typical 60-80Kbps)	All 2G features plus: • MMS (Multimedia Message Service) • Web browsing • Real-time location-based services such as directions Basic multimedia, including support for short audio and video clips, games and images
	GPRS	Up to 114Kbps (30-40Kbps)	
	HSCSD	Up to 64Kbps	
	EDGE	Up to 384Kbps	
	WiDEN	Up to 100Kbps	
2.75G	EGPRS 2	473Kbps (uplink) to 1.2Mbps (downlink)[2]	Better performance for all 2/2.5G services
3G (DSL speeds)	CDMA2000 EVDO (data only) Rev 0	Up to 2.4Mbps	Support for all 2G and 2.5G features plus: • Full motion video • Streaming music • 3D gaming • Faster Web browsing
	CDMA2000 EVDV (simultaneous voice and data)	Up to 2.4Mbps	
	UMTS	Up to 2Mbps	
	WCDMA	Up to 2Mbps	
	CDMA2000/ EVDO-Rev A	Up to 3.1Mbps	
3.5G (cable speeds)	HSDPA	Up to 14.4Mbps	Support for all 2/2.5/3G features plus: • On-demand video • Video conferencing • Faster Web browsing (especially graphics intensive sites)
	CDMA2000/ EVDO Rev B	Up to 46Mbps	
4G (wired networking equivalent)	WiMAX	100+Mbps	Support for all prior 2G/3G features plus: • High quality streaming video • High quality videoconferencing • High quality Voice-over-IP (VoIP)
	UMB	35Mbps	
	LTE	100Mbps	

Reflects evolution of CDMA network Reflects evolution of GSM network

Слика 10: Основне карактеристике мобилних мрежа

2G дигиталне мреже су се појавиле 90-тих година прошлог века: GSM (Global System for Mobile Communications, оригинално Groupe Spécial Mobile) стандард у Европи и CDMA (Code Division Multiple Access) у САД. Са увођењем ових мрежа и њиховом даљом еволуцијом ка 4G мрежама расте брзина преноса података а самим тиме и број имплементираних сервиса. Такође, омогућен је приступ Интернету и сви његови сервиси – почела је ера smart phone-ова. На слици 10. је дат преглед карактеристика аналогних и дигиталних мобилних мрежа.

9. БЕЗБЕДНОСНИ РИЗИЦИ КОРИШЋЕЊА МОБИЛНИХ ТЕЛЕФОНА

Радио-мобилне мреже су због своје природе и окружења веома изложене злонамерним нападима. Протоколи за мобилну комуникацију су тако пројектовани да обезбеде широку комуникацију и висок пропусни опсег. Међутим, због недостатака фреквенцијског спектра, примењени протоколи користе ограничене ресурсе. Поред тога, због природе безбедносних проблема, ови протоколи нису у стању да обезбеде адекватне механизме заштите, што с друге стране омогућава приступ хакерима. Сервиси у мобилној телефонији су у данашње време веома комплексни и подразумевају примену апликација које користе велике групе корисника, па су самим тиме интеракције међу њима (н.пр. јавне и безбедносне службе, банкарство ит.д.) структурално веома сложене и због потребе непрекидне дистрибуције информација осетљиве на безбеддносне претње.

Последњих година бележи се пораст напада на “smart” телефоне. Током 2011. године корисници широм света оштећени су за укупно 110 милијарди долара. По статистици 1 од 5 мобилних терминала је нападнут, а степен рањивости је достигао 93%. Напади на мобилне уређаје могу се сврстати у следеће:

- злонамерни софтвер (malware),
- директни напади,
- физички напади и
- пресретање података, прислушкивање и „цурење“ информација.

9.1. Malware и директни напади

Као што смо рекли, данашњи мобилни терминали су уједно и компјутери, али проблем је што углавном немају инсталиране: антивирусе, firewall-ove, нити шифровање података као што је примењено код персоналних рачунара. Самим тим су више изложени нападима преко Интернета.

Мобилни телефон се може „заразити“ приликом скидања и инсталирања софтвера за мобилни терминал (као што су бесплатне апликације на Интернету које могу скривати вирусе), преко анкета за освајање награда, приступа зараженим сајтовима, „скидањем“ игрица са Интернета...

Вирус у мобилном терминалу може нападачу да омогући приступање подацима које корисник има: именик, поверљиви подаци, e-mail, password-и... Вирус може да наложи телефону да шаље лажне наградне поруке које се тарифирају, корисник то не види, а наплата се додаје на његов рачун. Данас су веома популарне друштвене мреже, а њихови корисници су мање опрезни, па на пример, ако корисник остави свој број мобилног телефона на профилу, његов телефон постаје лака мета напада. Такође, вирус може бити присутан на сајту банке: држи отворену сесију чак и кад се корисник излогује, нападач преузме token и представи се као власник рачуна.

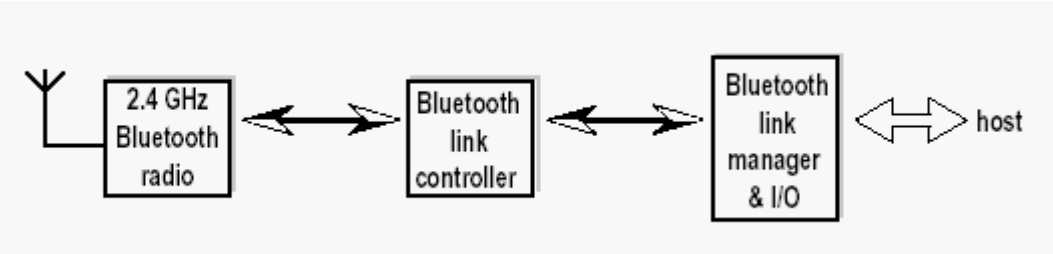
9.2. Физички напади

Предност мобилних терминала су мале димензије и лака преносивост, које омогућавају мобилност корисника. Али, из истог разлога телефони су више доступни за крађу. Корисници на својим “паметним” телефонима често имају поверљиве приватне и пословне информације, стога је потребно увести одређене мере заштите: password за приступ мобилном терминалу, back-up података на PC, избор провајдера који омогућава даљинско брисање података из телефона...

9.3. Пресретање података, прислушкивање и цурење информација

9.3.1. Напади преко Bluetooth интерфејса

Bluetooth је показао бројне проблеме по питању сигурности, осетљив је на нападе: прислушкивање, man-in-the-middle и одбијање сервиса. Када је Bluetooth укључен терминал је видљив за окружење и постаје потенцијална мета напада. На слици 11 је дата блок шема Bluetooth система.



Слика 11: Функционални блокови Bluetooth система

Најпознатији Bluetooth напади су:

- Bluesnarfing – ови напади подразумевају приступ телефону преко Bluetooth интерфејса ради откривања информација као што су адресе, ставке из календара или чак идентитета самог телефона (International Mobile Equipment Identity).

- Bluebugging – омогућава хакерисање телефона ради коришћења његових команди чиме се омогућава прислушкивање телефонских разговора, слање и примање текстуалних порука, па чак и повезивање са Интернетом.

- Denial of service (DOS) – нападач користи свој уређај и тражи константно упаривање са уређајем који напада са циљем стварања сметњи, односно рушења сервиса и основних функција телефона.

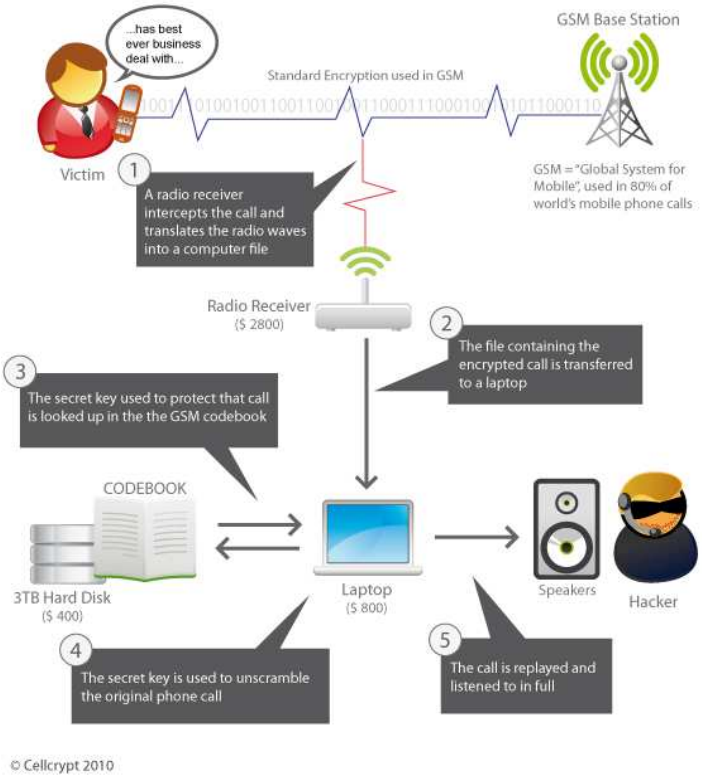
9.3.2. Напади преко Wireless мреже

Када је реч о Wireless мрежама, нападач нпр. може да конфигурише свој рачунар тако да се представља као приступна тачка Wi-Fi hotspot-a у кафићу или на аеродрому. Када нападач направи hotspot тако да мобилни корисник детектује јак сигнал врло је вероватно да ће имати много мета за напад. Компјутер може да рутира саобраћај до легитимног access point-a док наставља праћење комуникације. На овај начин може доћи до врло поверљивих информација као што су банковни рачуни и шифре корисника. (На сличан начин, али и доста тежи, могуће је представити се као легитимна базна станица крајњем кориснику и преузимати податке и тарифирати саобраћај.)

9.3.3. Прислушкивање

Кад је реч о прислушкивању поред опреме за прислушкивање разговора мобилних преплатника најједноставнији начин је инсталирање посебног софтвера у мобилни терминал који нападач жели да прислушкује. Тај софтвер прикупља и прослеђује информације на други телефон или сервер. Уз то, постоје апликације на телефону које омогућавају удаљено укључивање микрофона и слушање и снимање разговора из окружења.
Обзиром да су криптографски алгоритми за шифовање у GSM мрежама слаба заштита (A5/1 и A5/2 алгоритми који се користе у 2G мрежама су деконспирисани, а за A5/3 који

се користи у 3G мрежама су објављени теоријски радови напада на исти) могућност прислушкивања се своди на прислушкивање без криптозаштите.
У овом случају постоје пасивни напади (Слика 12.) који се своде на пријем сигнала између телефона и базне станице, без приступа истим, и његово декодовање помоћу одговарајућег софтвера, пријемника и антене и активни напади где се нападач представља као најближа легална базна станица и посредује у саобраћају кроз мрежу користећи опрему чија вредност не прелази 1500 америчких долара.



Слика 12: Шема пасивног напада на мобилни телефон

9.3.4. „Цурење“ информација

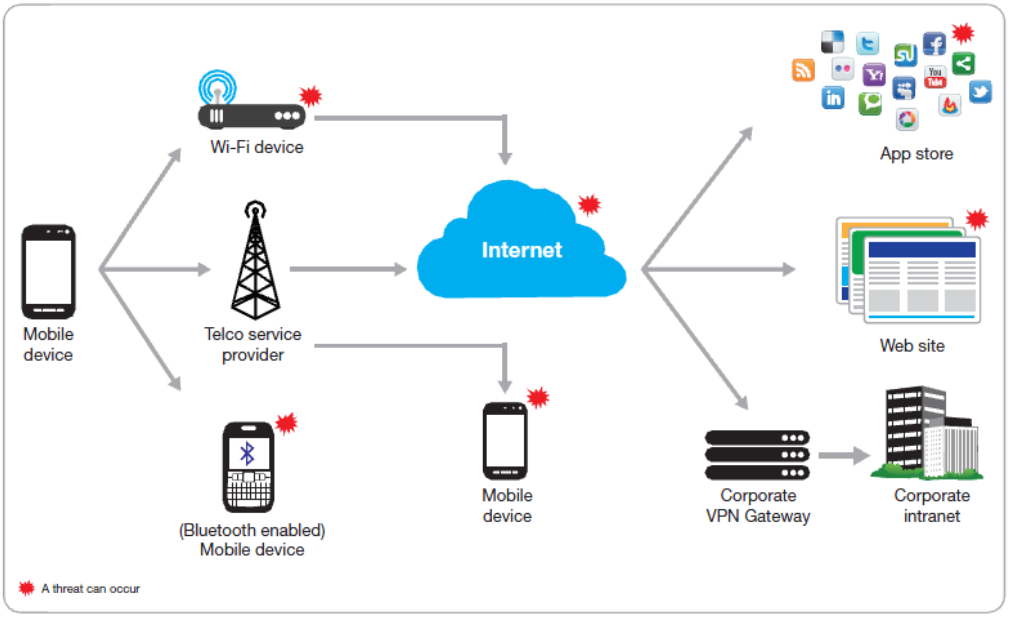
Са релативно јефтином опремом (око 1000 долара) нападач може добити крипто кључеве из мобилног уређаја (smart телефони и таблети) анализирајући EM емисију са процесора. Сви уређаји имају ту слабост независно од произвођача и типа оперативног система. У ту сврху се на мобилном терминалу искључе све опције: 3G, 4G, WiFi, Bluetooth...(airplane mod), како би се доказало да се цурење информација посматра са ненамерне EM емисије са процесора, а не са ових RF сигнала. Врло скромна опрема је потребна нападачу (сонда, Yagi антена, пријемник и дигитализатор) да би на краткој удаљености (до 2м) од мобилног телефона могао да нападне и открије кључеве. Забрињавајуће је да слични напади могу да се реализују на мобилне уређаје који користе NFC (Near Field Communication) за плаћање.

9.4. US-CERT препоруке

Имајући у виду горе исказане безбедносне претње US-CERT (United States Computer Emergency Readiness Team) је израдио следеће препоруке за умањење безбедносног ризика за коришћење мобилних телефона:

- Одржавати ажурним оперативни систем и сав кориснички софтвер на телефону;
- Инсталирати анти-вирусни софтвер и одржавати га ажурним;

- Ако је доступна, активирати аутентикацију PIN-ом или лозинком за приступ телефону;
- Шифровати личне и осетљиве податке, када је то могуће;
- Деактивирати Bluetooth, infrared, и/или Wi-Fi, када се не користе;
- Поставити Bluetooth-enabled devices у non-discoverable мод како би био невидљив за неаутентификоване уређаје;
- Бити опрезан приликом оварања електронске поште и attachment-а уз текстуалне поруке, као и понуђених линкова;
- Избегавати приступ непознатим Wi-Fi мрежама;
- Обрисати све информације са телефона пре његове замене и
- Одржавати на високом нивоу свест о безбедносним ризицима коришћења мобилних телефона.

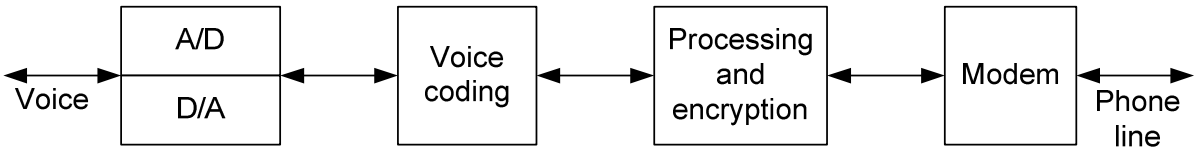


Слика 13: Приступне тачке за безбедносне претње у мобилној телефонији

10. ПРИНЦИП ОБРАДЕ ГОВОРНОГ СИГНАЛА

Шифровање говорних информација се своди на шифровање података, али је пре тога неопходно извршити обраду говорног сигнала у смислу припреме за шифовање и прилагођења капацитету комуникационог канала, без обзира да ли се ради о преносу информација путем жичних или бежичних веза, односно да ли се ради о фиксној (аналогној или дигиталној) или мобилној телефонији.

Принцип обраде ће бити објашњен на примеру обраде говорног сигнала у фиксној аналогној телефонији (слика 14).



Слика 14: Обрада говорног сигнала

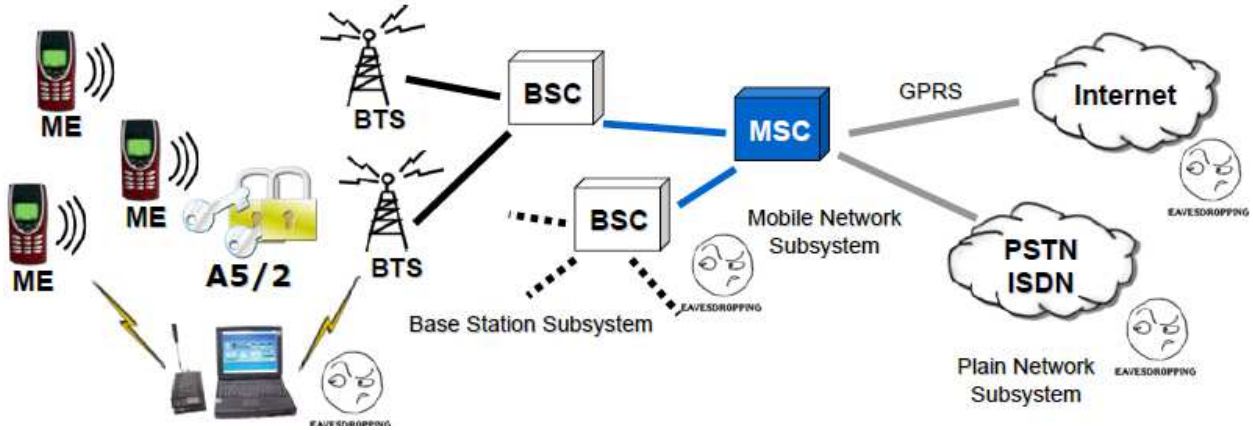
Говорни сигнал из микрофона (аналогни сигнал) се прво дигитализује A/D конвертором. Дигитални сигнал на излазу из A/D конвертора је 64 kb/s. Да би било могуће информацију о говору пренети кроз телефонски канал потребно је редуковати битску брзину. Вокодер редукује брзину у опсег 2400 - 9600 b/s задржавајући особине говорног сигнала.

Процесор прихвата дигиталну информацију вокодера и врши додатну обраду да би информација била спремна за слање на линију. Овде се врши заштита информације и пакетирање података. Модем прихвата податке од процесора и одговарајућим поступцима модулације претвара у аналогни сигнал који се налази у опсегу 300 - 3400 Hz који је могуће послати кроз телефонске линије.

У глави која следи би ће приказана нека од савремених решења за криптозаштиту мобилне телефоније, која се у принципу своде на већ познете принципе заштите у фиксној телефонији, уважавајући специфичности коришћења мобилних телефона у односу на фиксне и мобилних бежичних комуникација, односно мрежа.

11. САВРЕМЕНА РЕШЕЊА ЗА КРИПТОЗАШТИТУ У МОБИЛНОЈ ТЕЛЕФОНИЈИ

У овом поглављу је дат преглед неких од познатих и јавно доступних решења за заштиту мобилне телефоније. Као што смо већ рекли, мобилне комуникације саме по себи нису довољно безбедне, поготово када се има у виду да се користи различита комуникациона преносна инфраструктура (Слика 15). GSM стандард који се користи у мобилној телефонији има имплементирану криптозаштиту која је јавно позната и слаба и може се лако пробити. Довољна је и једна тачка рањивости система да дође до компромитације безбедне комуникације.



Слика 15: Илустрација комуникационо преносне инфраструктуре

11.1.Compnautica

11.1.1. Концепт решења за заштиту

Compnautica је холандско-немачка приватна фирма која се бави решењима за безбедну комуникацију у информатичко-комуникационим системима.

У решењу овог произвођача остварује се криптозаштита говора, SMS и фајлова с краја - на крај (end-to-end); говор се трансформише у податаке, пакети података се шифрују и шаљу путем комуникационе инфраструктуре до пријемне стране телефона где се дешифрују.

Решење је применљиво у следећим мобилним мрежама: GSM, UMTS, GPRS, EDGE, CDMA, Wi-Fi, Satellite.
Решење криптозаштите које је имплементирано је у потпуности софтверско и применљиво је за следеће оперативне системе:

- Windows Mobile,
- Linux,
- Symbian,
- BlackBerry (fist customer shipments Q1 2011) и
- Android (release 3G in Q2 2011).

Compumatica је развила два система за сигурну комуникацију који се разликују у типу комуникације: **Compumatica GSM** који ради на GSM мрежама и користи CSD канал за пренос података брзине од 9,6 kb/s преко GSM мреже и **Compumatica 3G** који користи мреже последње генерације као што су UMTS, HSDPA, EDGE, GPRS као и Wi-Fi.

CSD (circuit switched data) је протокол за асинхрони пренос података кроз GSM мреже на брзинама 9600/14,400 b/s. Постоје два типа CSD протокола: ITU-T V.32 - аналогни и V.110 - дигитални. Неке GSM мреже не дозвољавају коришћење CSD за припејд кориснике, па је пожељно бити постпејд корисник. Такође у неким земљама се подразумева коришћење CSD у оквиру GSM сервиса, док се у другим та услуга посебно захтева и плаћа. Под тим условима, препоручује се да се од провајдера затражи додела другог броја (data number) како би се умањили проблеми у рутирању data позива, поготово када сте у ромингу.

Безбедност решења се заснива на:

- "С краја на крај" (end-to-end) шифровању говора и података и преноса у шифрованом формату где се на пријемној страни врши дешифровање.
- За шировање се користи стандардни јавни блоковски криптографски алгоритам AESдужине кључа од 256 бита. AES (Advanced Encryption Standard) је блоковски криптографски алгоритам описан у публикацији FIPS PUBS (Federal Information Processing Standards Publications) 197 америчког националног института за стандардизацију, National Institute of Standards and Technology (NIST). На захтев се могу имплементирати и остали јавни алгоритми, као и сопствена криптолошка решења.
- KMS (Key Managament System) систем за генерисање и дистрибуцију кључева. На захтев, могућа је криптолошка модификација KMS.
- Дистрибуција симетричних кључева обезбеђује високу безбедност од "man-in-the-middle" напада.
- Elliptic Curve Diffie-Hellmann 571 битни протокол, који се базира на примени елиптичких криви у криптографији, се користи за размену кључа (сесијског) и у комбинацији са унапред дистрибуираним кључевима обезбеђује високу безбедност.

11.1.2. Compumatica SMS

Ово решење је предвиђено само за заштиту порука и има следеће карактеристике:

- мени заштићен лозинком (Слика 16)

- AES 256 алгоритам за шифровање SMS порука,
- могућност ручног уноса кључева за шифровање или коришћење аутоматски генерисаних,
- могућност слања такозваних Flash crypto SMS које се аутоматски бришу након шифровања,
- маогућност аутентикације за читање и писање SMS,
- крипто-именик и могућност формирања затворених група корисника,
- аларма за неауторизовану замену SIM картице кроз SMS поруку која садржи GPS координате за локализацију телефона.



Слика 16: Илустрација графичког интерфејса апликације за шифровање SMS

11.1.3. Расположиви модели телефона

Избор расположивих мобилних телефона зависи од оперативног ситема и типа комуникационе мобилне мреже.

За оперативни систем Windows Mobile OS:

- Compu(matica) GSM: HTC Touch Viva
- Compu(matica) 3G: HTC Touch 3G, Touch Pro, Touch Pro II, TytnII, Cruise, Diamond, Diamond II, Snap, 740, Touch2, HD, HD2 , Sony Ericsson Experia.

За оперативни систем Linux:

- GSM QuadBand телефон (Слика 17), оперативни систем инсталиран од стране фирме Compumatica, код кога су GPRS, Bluetooth, камера и multimedia искључени из сигурносних разлога.



Слика 17: GSM QuadBand телефон

За оперативни систем Symbian:

– Compu(matica) GSM и 3G: Nokia E51, E63, E71, E66, N81, N82, N95, E90, E52, E55, E71x, E72, E75, N85, N96

11.1.4. Secure BlackBerry (Compumatica BB)

Решење је развијено за 3G BlackBerry са OS 5.0 и 6.0. и има следеће карактеристике:

– решење се базира на μSD картицама са хрдверски имплементираном криптозаштитом,

– end-to-end енкрипција, интероперабилност са свим Compumatica 3G решењима базираним на оперативним системима Windows Mobile, Symbian и Android,

– комуникација са PSTN мрежом коришћењем Compumatica Gateway,

– висок квалитет говора

– могућност управљања кључевима посредством KMS,

– коришћење VoIP сервера који није укључен у енкрипцију,

– могућност криптозаштите SMS и e-Mail и т.д.

11.2.GSMK

GSMK (Gesellschaft für Sichere Mobile Kommunikation) је немачка фирма из Берлина која се бави заштићеним мобилним комуникацијама. У даљем тексту ће бити приказана нека од њихових решења за Кз мобилне телефоније.

11.2.1. Концепт примењене криптозаштите

Концепт решења за заштиту се заснива на следећим карактеристикама:

– криптозаштита говора и SMS,

– AES256 и Twofish алгоритми за шифровање,

– 4096 битни Diffie-Hellman протокол за размену кључева са SHA256 hash функцијом,

– заштита од неауторизованог приступа,

– доступан source cod за независну анализу.

11.2.2. Расположиви модели телефона

Први од GMSK уређаја је **GSMK CryptoPhone 300** (слика 18) који је намењен за GSM мреже и ради под оперативним системом WM5 који је развио произвођач.
Следећи модел **GSMK CryptoPhone 301** приказан на слици 19 је истих комуникационих и криптолошких карактеристика, али са побољшаном верзијом оперативног система WM 6.1.
Модел **GSMK CryptoPhone 400** (слика 20) IP је мобилни телефон са криптозаштитом намењен је за рад у GSM, 3G и WLAN мрежама и ради под оперативним системом WM 6.5.



Слика 18: GMSK CryptoPhone 300



Слика 19: GMSK CryptoPhone 301



Слика 20: GMSK CryptoPhone 400

11.2.3. GSMK CryptoPhone CUG

GSMK CryptoPhone CUG (Closed User Group) је систем који омогућава формирање затворених група корисника са сопственим 256-битним групним кључем (унутрашњи кључ). Сесијски кључ за сваки позив унутар групе корисника се размењује путем Diffie-Hellman протокола за размену кључева. Помоћу система је могуће формирати више група корисника, с тим што један корисник може партиципирати у више затворених група, чиме се омогућава вишехијерархијско планирање мреже.

Након планирања мреже, за сваког корисника се учитавају параметри генерисани системом преко конзоле (Key Management Console), односно рачунара (слика 21) на коју је инсталиран систем.



Слика 21: Key Management Console

11.3.Casper Technology

Casper Technology (CasperTech) је италијанска (Торино) фирма која има сопствена решења за криптозаштиту мобилне телефоније у GSM и 3G мрежама, која ће бити приказана у даљем тексту.

11.3.1. Cryptech 2G

Cryptech 2G мобилни телефон (слика 22) за заштиту говора и SMS ради на GSM мрежама и користи CSD канал (слика 23) за пренос шифрованих порука. Шифровање се врши коришћењем стандардног AES256 криптографског алгоритма, док се за размену сесијских кључева користи Elliptic Curve Diffie-Hellmann 571-битни протокол. Решење за заштиту ради под оперативним системима Windows Mobile, Symbian и Linux.



Слика 22: Cryptech 2G мобилни телефон

Решење је доступно на Nokia Symbian S60 FP1 и FP2, HTC Windows Mobile и Linux мобилним телефонима.



Слика 23: Криптозаштићена GSM мрежа

11.3.2. Cryptech Linux

Cryptech Linux мобилни телефон (слика 24) је такође предвиђен за рад у GSM мрежама, а за енкрипцију користи AES256 или криптографски алгоритам дефинисан од стране клијента. За размену сесијских кључева користи се Diffie-Hellman 4096-битни или Elliptic Curve Diffie-Hellmann 571-битни протокол.

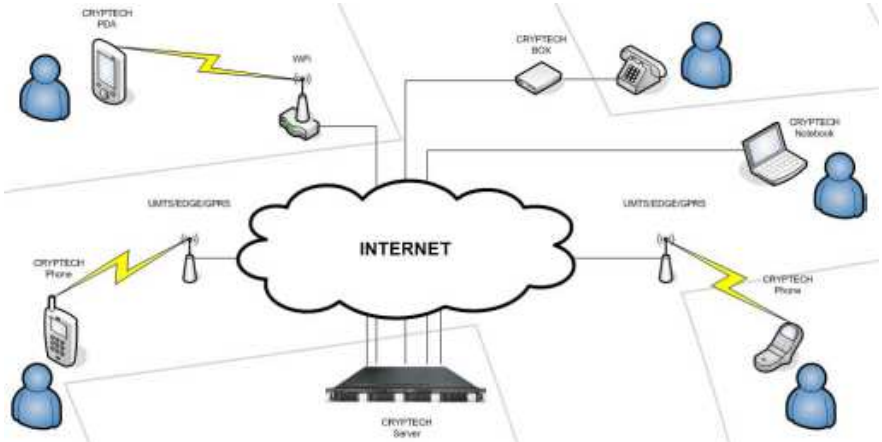
Кључеви (унутрашњи кључ) се могу директно генерисати и уносити од стране корисника или преко KMS (Key Management System).



Слика 24: Cryptech Linux мобилни телефон

11.3.3. Cryptech 3G

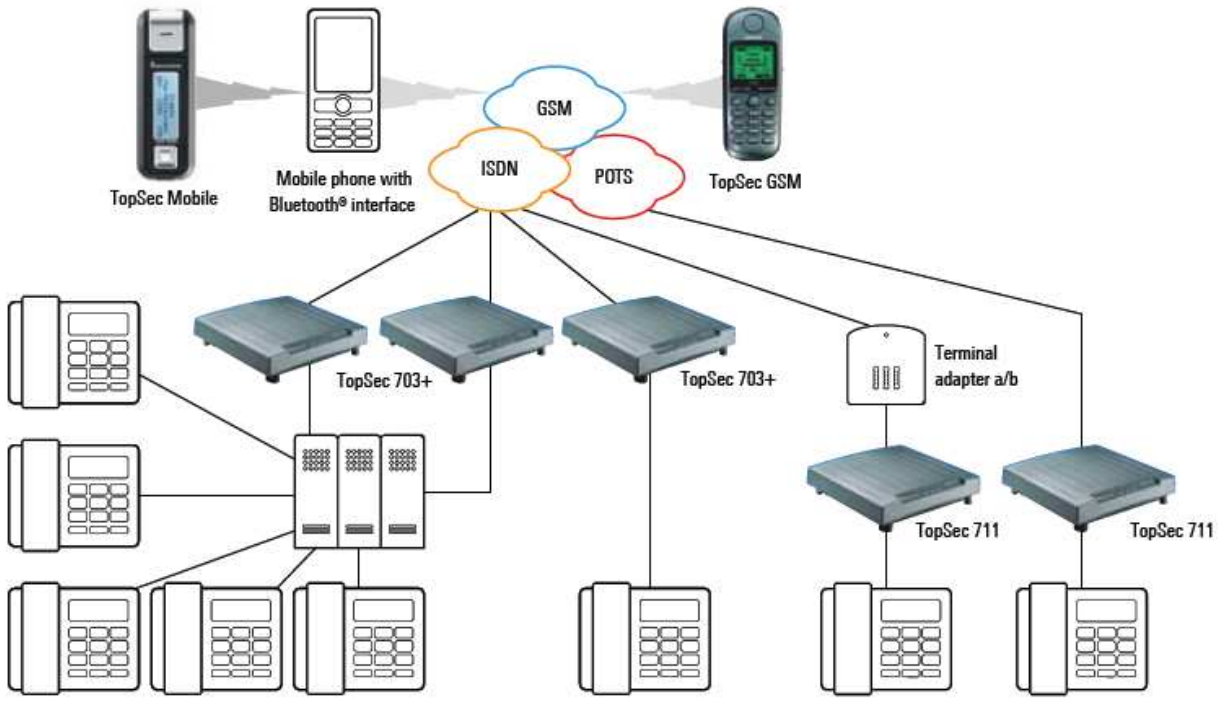
Cryptech 3G мобилни телефон за заштиту говора и SMS ради преко GSM, EDGE, GPRS, WCDMA, UTMS, HSDPA, HSUPA, WiFi и Satellite мрежа. Криптолошке карактеристике су му као код претходно описаног решења. Илустрација рада у 3G мрежи дата је на слици 25.



Слика 25: Илустрација рада у 3G мрежи

11.4.Rohde & Schwarz

Rohde & Schwarz је позната немачка фирма, која поред осталог производног програма има и решења из свих области криптозаштите информација, па тако из области криптозаштите мобилне телефоније. Решења за заштиту мобилне телефоније представљају део производа TopSec Product family за заштиту говора у алналогним, дигиталним и мобилним радио мрежама (слика 26).



Слика 26: Криптозаштита у аналогним, дигиталним и мобилним радио мрежама

11.4.1. TopSec GSM encrypting mobile phone

Овај телефон (Siemens S 35i) служи за криптозаштиту говора у GSM мрежама и у себи има интегрисани криптомодул (слика 27). За пренос шифрованих порука телефон користи data канал (CSD) са брзином преноса података од 9600b/s. Говорна информација се пре шифровања дигитализује и компресује са вокодером.



Слика 27: Криптомодул TopSec GSM

11.4.2. TopSec Mobile voice encryption device

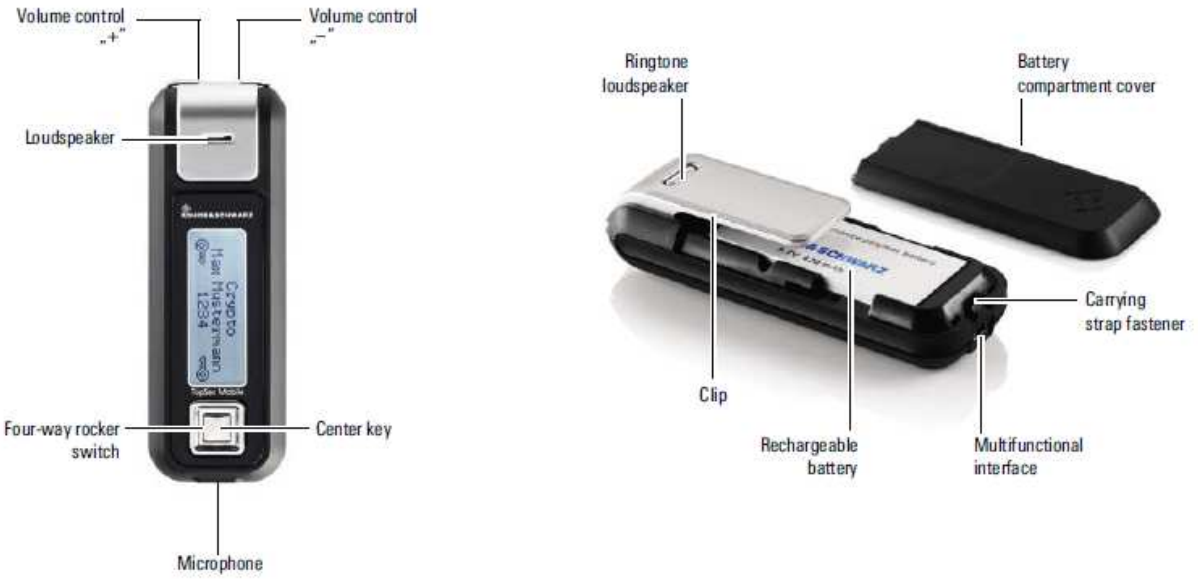
TopSec Mobile представља уређај за криптозаштиту говора и опремљен је са Bluetooth интерфејсом. Овај уређај се не везује директно на комуникациону мрежу, већ преко комуникационе терминалне опреме као што је на пример мобилни телефон. Уређај може да оствари везу са било којим мобилним телефоном који има Bluetooth интерфејс.

Ово решење за заштиту има две главне предности у односу на сва горе наведена:

– није везано за одређену мобилну радио мрежу и

– омогућава слободу у избору типа мобилних телефона.

Осим енкрипционе компоненте, уређај поседује микрофон, звучник, дисплей и одређене тастере (слика 28).



Слика 28: Уређај TopSec Mobile

11.4.3. Криптолошки концепт

TopSec Mobile користи 1024-битни RSA алгоритам за размену кључева и 128-битни AES симетрични алгоритам за заштиту поверљивих информација, односно у новијој верзији уређаја RSA 2048 и AES-256.

Уређај користи Diffie-Hellman-ов протокол за размену сесијских кључева при сваком позиву, што омогућава успоставу заштићене комуникације без потребе за постојањем треће стране у комуникацији. С обзиром да се наведени протокол базира на систему са јавним кључевима, приватни и тајни криптолошки параметри инсталирају се у уређај у процесу производње и као такви се испоручују заједно са уређајем.

После успешне успоставе заједничког сесијског кључа, сви тајни параметри коришћени од стране Diffie-Hellman-овог протокола се бришу из уређаја. Сесијски кључ се брише након раскида успостављене везе.

Да би се омогућила детекција и спречио напад типа man-in-the-middle, уређај генерише четвороцифрен број који се по успостави везе приказује на дисплеју. Тај број мора бити идентичан код оба уређаја која учествују у комуникацији.

Осим тога, могуће је креирати и затворене групе корисника. Да би се то остварило потребно је постојање треће стране од поверења. Ту страну у фамилији TopSec уређаја представља такозвани TopSec Administrator, који додељује сертификате уређајима. На основу добијеног сертификата врши се аутентикација уређаја приликом успоставе везе.

Од пропратног софтвера, уз уређај се добија софтвер TopSec Mobile PhoneBook Editor који служи за рад са телефонским именником. Наиме, TopSec Mobile врши заштићени позив тако што се из телефонског именика уређаја одабере број, односно особа која се позива (не може се позивати произвољни број, већ само број који смо претходно унели у именик). С обзиром на спорији и заморнији начин уноса записа у телефонски именик директно са уређаја, произвођач даје софтвер којим се телефонски именик ажурира на рачунару, а потом помоћу USB кабла “спушта” у уређај.

11.4.4. TopSec Mobile за smartphone и laptop

Ово је најновија верзија уређаја TopSec Mobile која обезбеђује криптозаштићену говорну комуникацију преко IP мреже (слика 30.).

11.4.5. Основне карактеристике

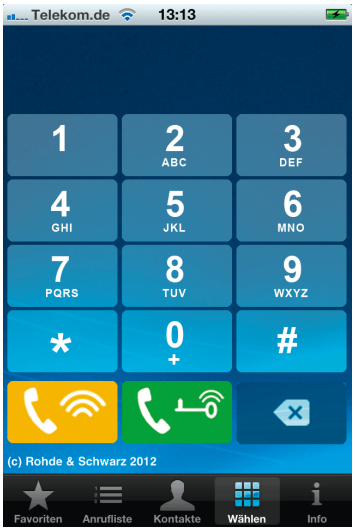
– Bluetooth интерфејс за конекцију са smartphon-ом или laptop-ом.

– USB кабал за конекцију са laptop-ом.

– TopSec Phone апликација (слика 29.) за smartphone и laptop.

– Конекција на IP мрежу преко smartphone-а, laptop-а или сателитског терминала.

– Call-setup преко јавних или приватних VoIP сервера.



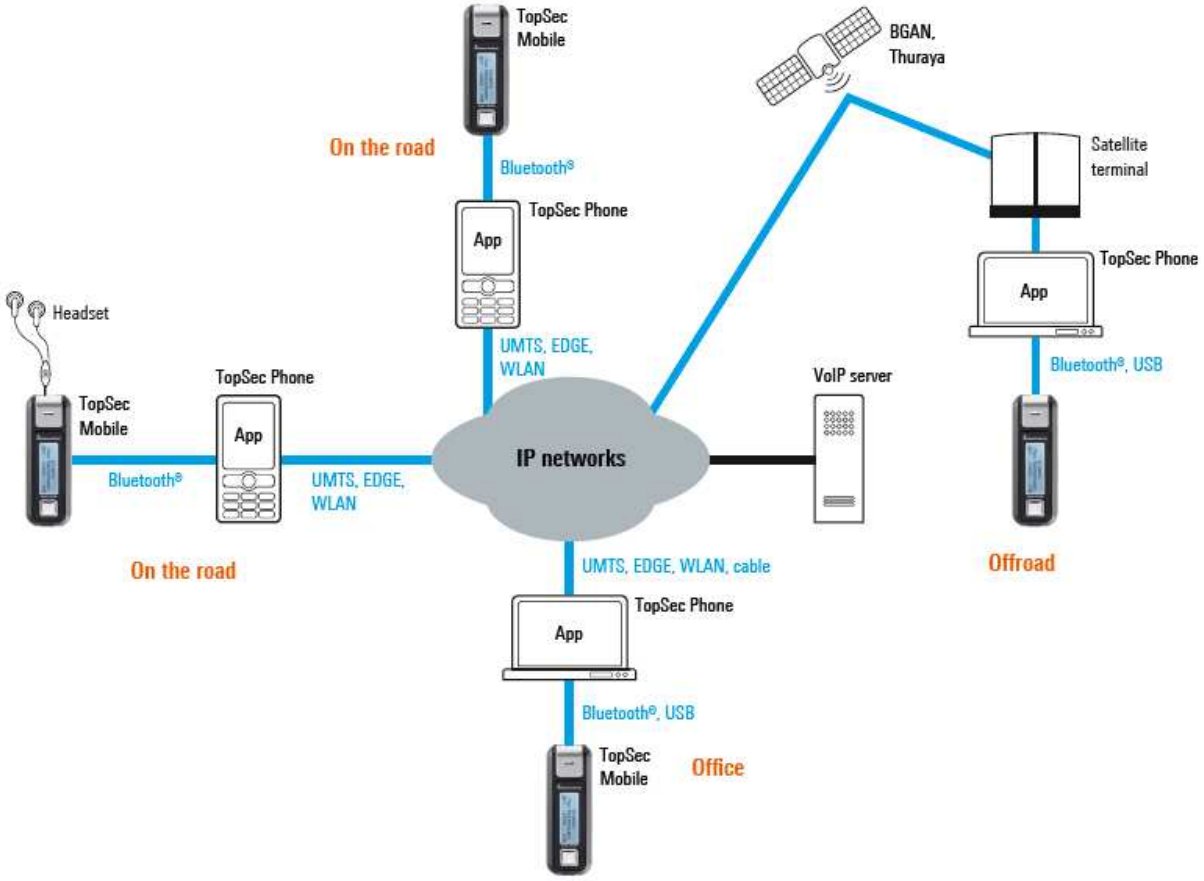
Слика 29: TopSec Phone апликација

11.4.6. Криптолошки концепт

– размена кључева са ECC DH 384-битни,

– аутентикација путем дигиталних сертификата,

– AES 256 енкрипција.



Слика 30: TopSec Mobile криптозаштита говора

11.5.Omnisec

Omnisec је швајцарски произвођач који нуди специјализовани криптозаштићени телефон Secure Mobile Phone Omnisec 230 (слика 31.) са прилагођеним оперативним системом Android.



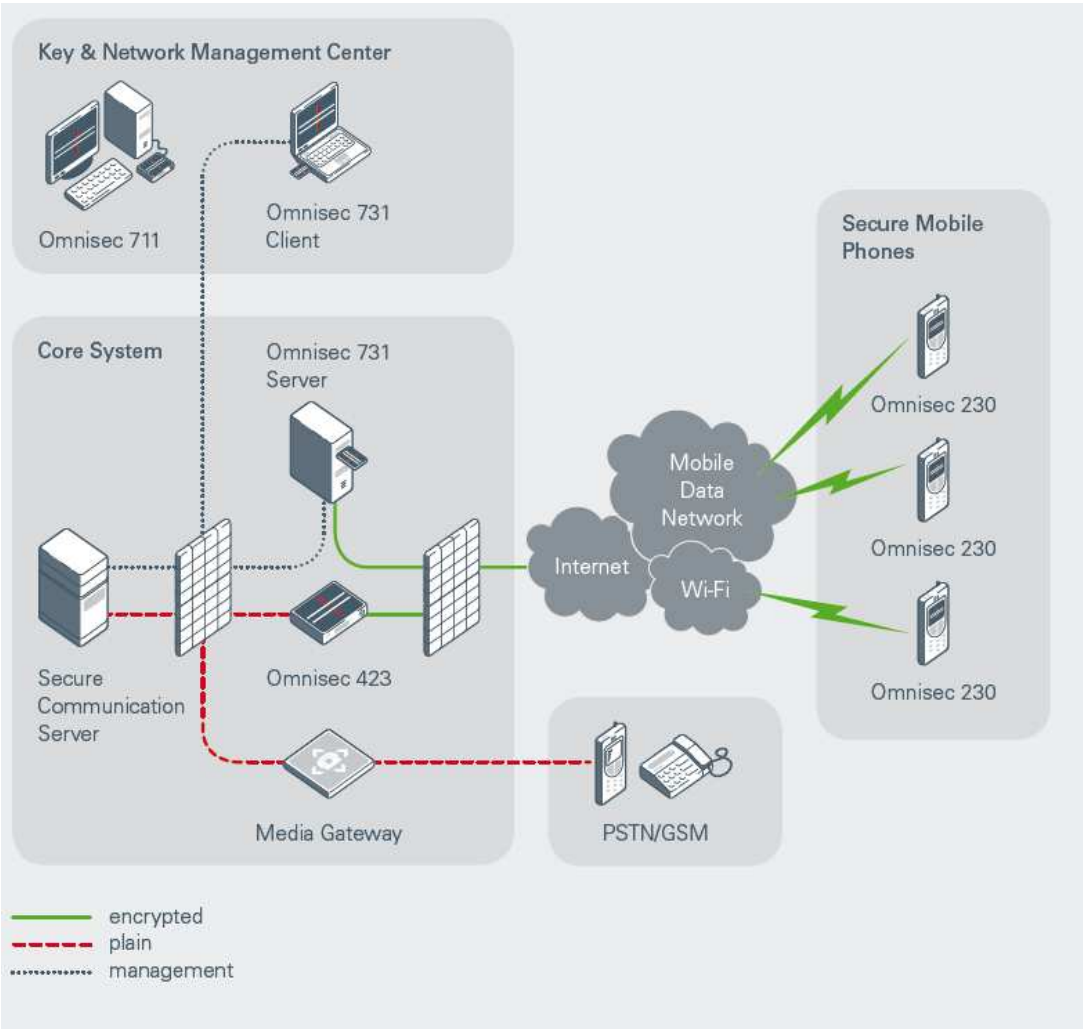
Слика 31: Secure Mobile Phone Omnisec 230

11.5.1. Основне карактеристике

– сопствени Android оперативни систем,
– UMTS Quadband (850 / 900 / 1900 / 2100 MHz),
– GSM / EDGE Quadband (850 / 900 / 1800 /1900 MHz).

11.5.2. Криптолошке карактеристике

– Omnisec 256-битни блоковски алгоритам, аутентикација Omnisec MAC,
– једнократна употреба сесијског кључа,
– мастер (унутрашњи) кључеви на микро SD картици,
– могућност верификације имплементираних криптолошких процедура и алгоритма,
– IPSec VPN успостава криптографских тунела,
– Secure Key Management Center (KMC),Omnisec 711, and Security Module Programmer, Omnisec 704,
– Security & Network Management Center (NMC), Omnisec 731,



Слика 32: Omisec решење за криптозаштиту говора

Omnisec-ово решење за криптозаштиту говора у мобилној телефонији (слика 32.) у основи чине: Кз мобилни телефон (Secure Mobile Phone Omnisec 230), систем за генерисање кључева (Secure Key Management Center (KMC), Omnisec 711), језгро система за мрежно и

безбедоносно управљање (Secure Mobile Core System) и комуникациона мрежа (Интернет, мрежа мобилне телефоније и/или Wireless мрежа).

Кз телефон је наменски телефон са модификованим Android оперативним системом. Телефон обезбеђује само заштићену комуникацију, односно није могуће позивање и говорна комуникација у отвореном режиму рада са корисницима ван криптозаштићене мреже. Криптографске функције (алгоритам и др.) су имлементиране у језгро оперативног система телефона, док се мастер кључ (кључеви) налази на сигурносном модулу (μSD картици, која се умеће у посебан слот телефона поред SIM картице).

Систем за генерисање кључева (КМС), на бази извора са белим шумом обезбеђује програмирање сигурносних модула, односно смештање мастер кључа у модул.

Језгро система за мрежно и безбедоносно управљање обезбеђује надзор над мрежом у комуникационом и безбедносном смислу. Могуће је обезбедити више (максимално 16) затворених група (мрежа) корисника (телефона), с тим што је дозвољено да један или више корисника буду у једној или више затворених мрежа.

Заштићена комуникација се обезбеђује формирањем IPSec VPN тунела између појединих Кз телефона и Кз уређаја за шифровање на IP нивоу (Omnisec 423) који се налази у језгру система. Са стране корисника приступ Интернету се обезбеђује преко мреже мобилне телефоније или wirelees-a.

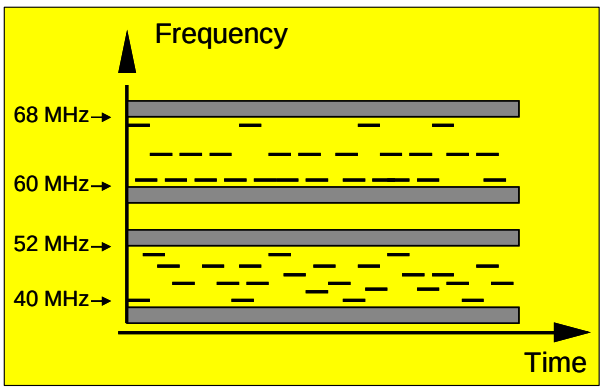
У језгро мреже могуће је прикључити, преко media gateway-a, и кориснике са јавне GSM или PTSN мреже, али је тада комуникација до језгра мреже незаштићена.

12. СПЕЦИФИЧНОСТИ ШИФРОВАЊА ГОВОРА У РАДИО КОМУНИКАЦИЈАМА

Радио комуникације (VHF, HF опсег) су посебно интересантне за употребу у војним тактичким (покретним) системима. Основни услови за безбедан пренос информација је испуњење захтева који се тичу заштите података приликом преноса (Communication Security - COMSEC) и заштите саобраћаја (Transport Security - TRANSEC).

Обзиром да потребу за заштитом података није потребно посебно образлагати, неопходно је објаснити потребу за заштиттом саобраћаја. Војне комуникације су под сталном опсервацијом обавештајних служби свугде у свету, како у смислу прислушкивања, тако и у смислу електронског ометања.

Један од механизама за заштиту саобраћаја је фреквенцијско скакање (енг. frequency hopping) у оквиру радио-фреквенцијског спектра (Слика 33.) по дефинисаним фреквенентним врендностима (каналима) и псеудослучајном реду дефинисаном криптографским алгоритмом и кључевима. За шифровање података користе се COMSEC кључеви, а за шифровање саобраћаја TRANSEC кључеви.



Слика 33: Диаграм фреквенцијског скакања у ВВФ радио опсегу

13. ПОЈАМ КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА

Код уређаја за шифровање информација штићена информација је присутна на улазу у уређај (када је у питању шифровање) или на његовом излазу (дешифровање). Затим уређај врши трансформацију тајне информације у шифрат који се преноси каналом везе, или инверзну трансформацију којом се шифрат враћа у првобитан облик. Приликом поступака трансформисања информације из једног облика у други долази до емитовања паразитне електромагнетске енергије која може бити u корелацији са штићеном информацијом.

Као што смо рекли, информација која се електронски обрађује и преноси изазива паразитно електромагнетско зрачење на самом уређају на ком се врши обрада или на транспортном медијуму. Део тог зрачења не носи никакав информативни садржај и представља само сметње, међутим, постоји и такво електромагнетско зрачење на основу чије детекције се може под одређеним условима доћи до података о садржају обрађиване или преношене информације - њега називамо **компромитујуће електромагнетно зрачење (КЕМЗ)**. Илустрација појаве КЕМЗ дата је на слици 34.



Слика 34: Ток сигнала компромитујућег електромагнетног зрачења

Систем за обраду информација, у наведеном случају, може бити извор ЕМ зрачења које може довести до „поништавања“ тајних операција (рецимо криптозаштите информација) које систем покушава да изведе. Овде под „поништавањем“ сматрамо да ЕМ зрачење система може садржати компоненте које ће представљати или отворену поруку или начин обраде те поруке.

Из наведених разлога, потенцијалном нападачу треба онемогућити (или бар отежати) долажење до информација на основу КЕМЗ кроз предузимање одређених мера заштите. Под заштитом од КЕМЗ подразумева се смањење електромагнетског зрачења које је у корелацији са информацијом која се обрађује на одређеном уређају.

Мере заштите се односе на заштиту (оклапање) од КЕМЗ самих уређаја за обраду или криптозаштиту информација т.ј. појединих склопова уређаја или заштиту простора (Фарадејеви кавези) у којима се уређаји налазе. При детекцији КЕМЗ и верификацији заштите од КЕМЗ потребно је користити софистицирану мерну опрему високих перформанси (аланализатори спектра, мерни пријемници и.т.д.) уз примену одговарајућих мерних метода. У страној литератури компромитујуће електромагнетно зрачење се друкчије назива TEMPEST (Transient ElectroMagnetic Pulse Engineering Standard Technology).

14. ЗАКЉУЧАК

У овом раду било је речи о безбедности и криптозаштити информационо-комуникационих система. На почетку рада приказана је методологија по којој је истраживање обављено што је поред осталог подразумевало предмет истраживања, циљеве и задатке истраживања, методе истраживања и истраживачке хипотезе.

Циљ овог рада је био да се укаже на безбедносне ризике и претње и одговор на исте кроз имплементацију безбедносних механизама криптозаштите у оквиру информационо-комуникационих система.

За заштиту су предложена решења која се базирају на хибридним системима за криптозаштиту, односно системима који комбинују симетричну и асиметричну криптографију ради утврђивања аутентичности, заштите интегритета, обезбеђења непорецивости и заштиту тајности, чија имплементација зависи од врсте и типа информација које се штите и OSI безбедносне архитектуре.

Повећање броја доступних сервиса које мобилни телефон пружа у директној је пропорцији са безбедносним ризицима којима је корисник изложен и који могу изазвати различите последице од губитка или деконспирације података, до нарушавања функционалности мобилног телефона и финансијских губитака.

Примена модерних криптолошких решења обезбеђује заштиту сервиса који се штите, међу којима је најважнији говорни сигнал.

Видели смо да у већини случајева (осим код R&S уређаја TopSec Mobile) решења за криптозаштиту се пројектују за одређене моделе мобилних апарата и оперативних система који су примењени у њима.

У раду није било речи ризицима који потичу од хардвера телефона, односно од фабричког софтвера (firmware) уграђеног у компоненте и евентуалног постојања bypass-a (backdoor, trap door) за имплементиране сигурносне механизме, што треба имати у виду приликом верификације безбедносних карактеристика уређаја.

Такође, објашњен је и појам компромитујућег електромагнетног зрачења, као појаве о којој се мора водити рачуна приликом обраде или криптообраде информација.

15. ЛИТЕРАТУРА

[1] Да ли сте сигурни да сте безбедни?, Бошко Родић, Горан Ђорђевић, Продуктивност, Београд, 2004.

[2] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, November 16, 2005.

[3] Rick Lehtinen, Computer Security Basics, 2nd Edition, O'Reilly, June 2006.

[4] Милан Николић, Практични аспекти заштите приватности корисника и безбедности електронских комуникационих мрежа и услуга у Србији, часопис "Телекомуникације", број 5.

[5] Recommendation X.800, Security Archicecture for Open Systems Interconnection for CCITT applications, International Telecommunication Union (ITU), 1991.

[6] Милан Марковић, Гордана Стојановић, Вишеслојна архитектура заштите и технологије дигиталног потписа у систему електронског пословања, 2005.

[7] Security of mobile communications, Noureddine Boudriga, CRC Press, 2010, USA.2F94

[8] Bluetooth And Its Interent Security Issues, SANS Institute 2003.

[9] Cyber Threats to Mobile Devices, US-CERT Technical Information Paper, 2010.

[10] Mobile Device Security—Emerging Threats, Essential Strategies, Juniper Networks, Inc. , 2011.

[11] 2011 Mobile Threats Report, Juniper Networks, Inc., 2012.

[12] RSA Security's Official Guide to Cryptography, Steve Burnett and Stephen Paine, Osborne/McGraw-Hill, 2011.

[13] Applied Cryptography, Bruce Schneier, 2 ed, Wiley, 1996.

[14] www.crypto.ch

[15] www.kongsberg.com

[16] www.rsa.com/rsalabs

[17] www.rohde-schwarz.com

[18] www.omnisec.ch

[19] www.compumatica.eu

[20] www.cryptophone.de

[21] www.caspertech.com