Säkerhet inom UMTS

Säkerhet inom IP-baserad mobiltelefoni

LUNDS
UNIVERSITET
Lunds Tekniska Högskola

LTH Ingenjörshögskolan vid Campus Helsingborg

Examensarbete:
Mohamed Koleilat

LTH Ingenjörshögskolan vid Campus Helsingborg
Lunds Universitet
Box 882
251 08 Helsingborg

LTH School of Engineering
Lund University
Box 882
SE-251 08 Helsingborg
Sweden

Tryckt i Sverige
Media-Tryck
Biblioteksdirektionen
Lunds Universitet
Lund 2007

Sammanfattning

Syftet med detta examensarbete är att ge en beskrivning av utvecklingen och säkerheten hos 3G vilket erbjuder överföring av text, bilder, röst, video och multimedia. I Europa heter standarden UMTS och har definierats av European Telecommunications Standards Institute (ETSI).

I första delen av arbetet beskrivs kortfattat en översikt av säkerheten inom GSM för att senare gå över till 3G som det mesta av arbetet består av. Detta omfattar en översikt över UMTS nätverk dess metoder och finesser så som abonnents identitets skydd, autentisering, ström chiffer för trafiken, användarens relation för styrning av data mm. Därefter beskrivs attacker som förekommer inom 3G. I den sista delen beskrivs kortfattat om framtida mobiltelefoni 4G (fjärde generationens mobiltelefoni system).

Nyckelord: GSM, UMTS, 3G standar, UMTS svaghet, 3G attack

Abstract

The purpose of this project is to give a description of the development and the security in 3G which supports transferring text, picture, voice, video and multimedia. In Europe it is called UMTS which was defined by European Telecommunications Standards Institute (ETSI).

In the first part of the report contains an overview of GSM security and later I go on to 3G which most of the report consists of, that includes UMTS network and its methods and features, such as subscriber identity confidentiality and authentication, stream ciphering of user traffic and user-related control data. Some attacks that exist within 3G are described. In the last part the future cell phone 4G (fourth-generation cellular communication system) is briefly described.

Keywords: GSM, UMTS, 3G standard, UMTS weakness, 3G attack

Förord

Denna analys är resultatet av mitt examensarbete på LTH Ingenjörshögskolan vid Campus Helsingborg. Rapporten har utförts under höstterminen 2007. Idén till denna analys kom efter en inspirerande kurs i datasäkerhet. Efter långa dagar och nätter av arbete på den här analysen är jag nöjd och det är skönt att jag nu är klar. Jag vill passa på att tacka de personer som har hjälpt mig på vägen.

Jag vill först tacka mina föräldrar som stött mig under hela utbildningens gång och nu inför denna analys.

Jag vill tacka Mats Lilja som har varit min examinator på Lunds Teknikiska Universitet vid Campus Helsingborg.

Jag vill tacka Ben Smeets som har varit min handledare på Lunds universitet.

Slutligen vill jag tacka alla personer som har varit till stor hjälp under mina studiers framskridande, speciellt de som är på Campus Helsingborg.

Mohamed Koleilat
Helsingborg 2007-06-20

1 Inledning

Mobiler användes mer och mer som en vardagsutrustning för de flesta människor. Tekniken kring mobiltelefoner har ständigt utvecklats och mobiltelefoner har fått fler funktioner än att bara ringa vanligt röstsamtal. Kampen mellan de stora företagen som strävar efter att implementera nya och effektiva funktioner är stor, dessutom så ökar efterfrågan efter nya mobiltjänster allt mer i framtiden då mobilen får allt större kapacitet och prestanda. Den mest växande tjänsten är mobila transaktioner, där man kan genom sin mobiltelefon utföra betalningar eller överföra pengar mellan konton.

Intrång i det mobila nätet för att skaffa sig information är alltid intressant för de obehöriga. Därför är säkerheten i dessa sammanhang mycket viktig både för mottagaren och användaren.

1.1 Mål

3G (tredje generationen) är en ny teknik i mobiltelefonsammanhang. Är man ansluten till 3G nät så har man möjlighet att samtidigt överföra både ljud och bild vid ett telefonsamtal. I dagens läge så kan man skicka och ta emot e-post, ladda ner musik och program och betala online. Säkerheten är en viktig del i den tredje generationens mobiltelefoni framför allt när man ska tillämpa tjänster som används över Internet.

Målet med denna analys är att få en överblick över 3G mobila säkerheten och intrång som kan förekomma och eventuella åtgärder som kan vidtagas

1.2 Innehåll

- En kort överblick över säkerhet inom GSM mobiltelefoni.
- En beskrivning hur säkerheten i tredje generationen har utvecklats.
- Nackdelar och fördelar som kan finnas i tredje generationen mobiltelefoni.
- Eventuella lösningar som har valts för att minska risken får intrång.
- En kort beskrivning för tänkbara nya mobilgenerationer.

2 GSM

GSM (Global System for Mobile communication) är en övergång från det analoga till det digitala telefonsystemet som används runt hela världen. Andra generationens trådlösa telefon GSM använder Time Division Multiple Access (TDMA) standard. I GSM överförs all data i digital form. GSM kan anses som det första digitala nätet för mobil telekommunikation och till skillnad från de analoga näten så kodas all kommunikation till digital form innan den sänds. GSM-systemet skiljer på användare och telefon. Användaren tilldelas en identitet i systemet vilken ligger lagrad på ett litet kort, kallat SIM. Kortet kan flyttas mellan olika GSM-telefoner vilket gör att ett abonnemang inte är knutet till en speciell telefon

2.1 System översikt

Figur 1, är i grunden en överblick av GSM.s mobilnät. Delar som berör säkerheten kommer att tas upp i den här rapporten.

- *Mobile Equipment (ME)* – ME refererar till en flyttbar (mobil) enhet som stöds av GSM system. En ME utan ett SIM kort kan inte användas i GSM system.

- *Subscriber Identity Module (SIM)* – Ett SIM är ett smart kort som införs i ME. Ett SIM kort köps av en leverantör med en viss telefonoperatör. Ett SIM kort innehåller följande information om abonnenten.

    - The International Mobile Subscriber Identity (IMSI), den unika abonnenten identifieras.
    - Säkerhets nyckel (Ki) och kryptografisk algoritm (A3) det används för att bekräfta SIM kortets ärlighet.
    - Temporärar data som TMSI, Kc och annan nätverksinformation.
    - Datatjänst som t.ex. språk alternativ mm.
    - Card Holder Verification Information (CHV1/CHV2), bekräftar användarens förbindelse med kortet och skyddar mot stulna SIM kort.

- *Mobile Station (MS)* – När ett SIM kort införs i en trådlös telefon, kan MS vara återkomlig i mobil nätverket.

- *Base Transceiver Station (BTS)* – BTS förbinder mobilenheten till nätverket över GSM Air Interface.

- *Base Station Controller (BSC)* – BSC kontrollerar en mängd av BTS. Har olika centraluppgifter. BSC och BTS bildar basstation undersystem.

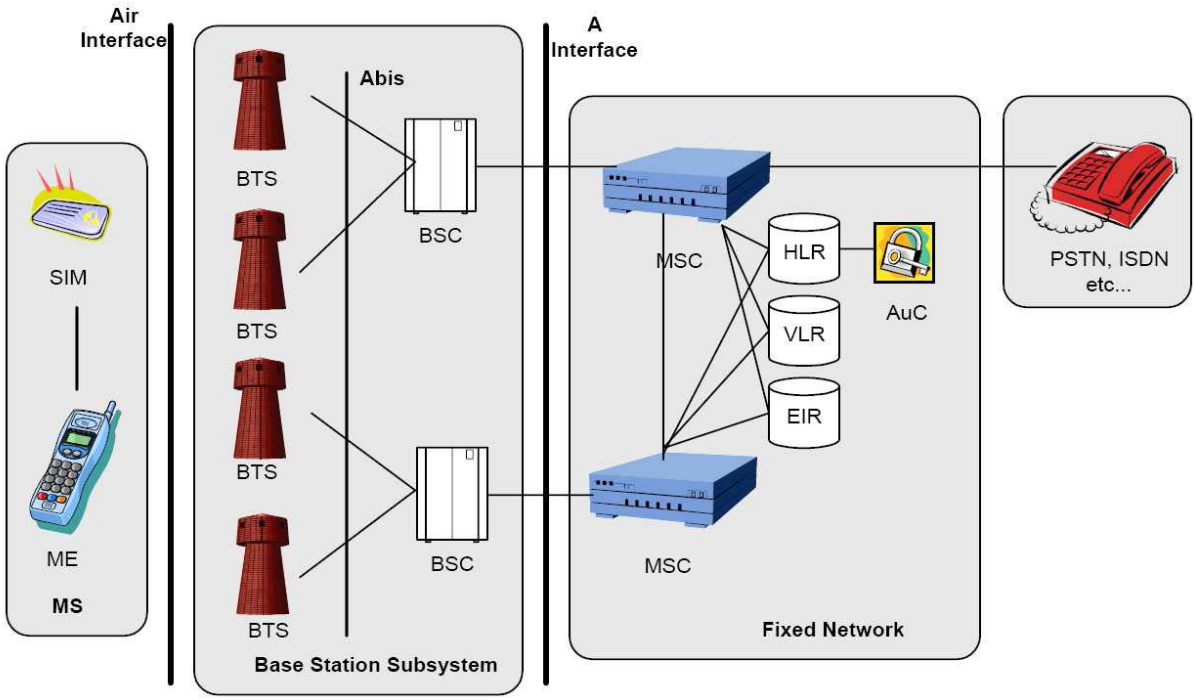
- *Mobile Switching Center (MSC)* – MSC kontrollerar många BSC. MSC består till stora delar av hårdvara som kan jämföras med en stor router.

- *Home Location Register (HLR)* – HLR lagrar abonnentens specifika data. När en GSM operator delar ut ett SIM kort till abonnenter, då lagrar operatorn en kopia av det väsentliga av SIM kortets information (Ki och IMSI) i HLR. Ki behålls hemligt för andra operatorer. Det måste existera en förändring i HLR för varje GSM nätverk för att betjäna operatorerna med autentiseringsparametrar.

- *Authentication Center* – Autentiserings Center (AuC) är ofta integrerad i HLR. Dess funktion är att beräkna autentiseringsparametrar.

- *Visitor Location Register(VLR)* – Ett lokaliseringsregister för besökare som liknar ett HLR, men endast för de abonnenterna som för närvarande vandrar omkring har en täckning inom VLR området. När en abonnent flyttar sig utanför VLR området, tar HLR hand om överföringen av abonnentens information från den gamla till den nya VLR. Varje MSC har en VLR men en VLR kan ha många MSCer.

- *Equipment Identity Register(EIR)* – Identitetsregister för hårdvara är nödvändigt för att förhindra stöld av ME. ME är ett attraktivt mål för tjuvar eftersom modellen inte har någon betydelse för dem, så länge det finns ett giltig SIM kort. En EIR kan användas som en svartlista för stulna eller förbjudna ME. En EIR har även en vitlista (med alla godkända ME) och en grålista (för att spåra en ME).



Figur 1: GSM arkitektur.

3 Säkerhet inom GSM

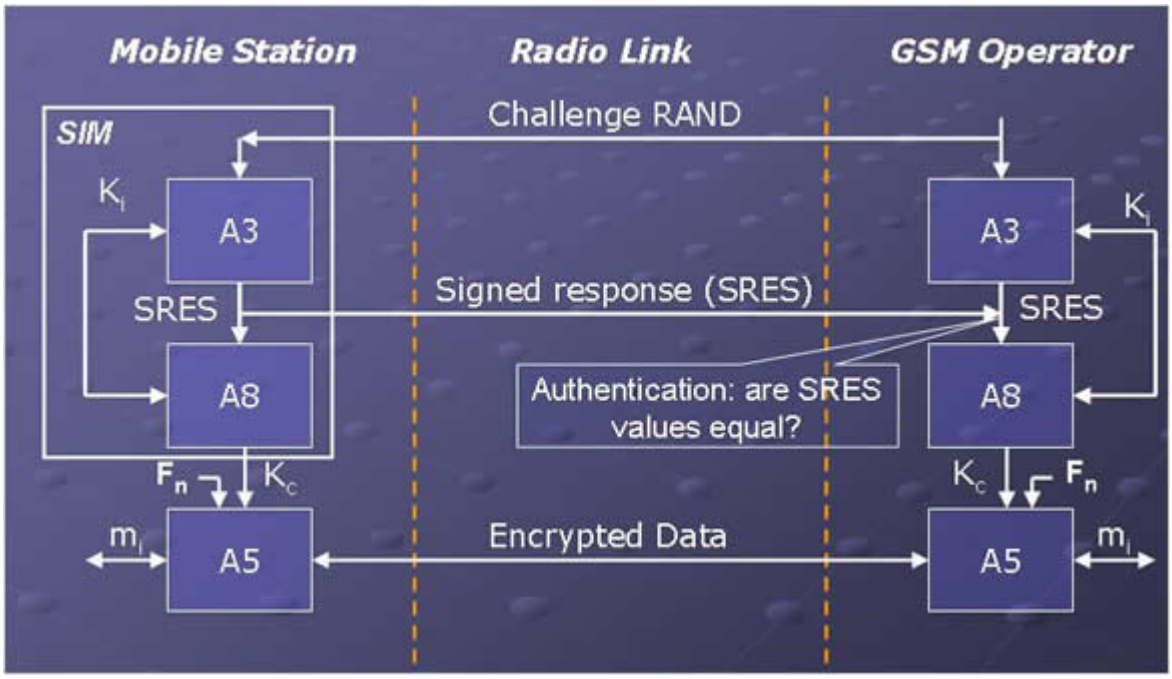
3.1 Mål

GSM säkerheten är nödvändigt för att skaffa hemlighållande och anonymitet över nätverket för användaren när ett samtal utförs, för att vara säker att nätverksoperator tar betalt för rätt användare och för att vara säker att operatörerna inte kollidera med varandra antingen av en händelse eller med flit.

3.2 Säkerhetsanvändning

Den första saken är att nätverket måste identifiera och autentisera användaren. För att utföra detta så skickar nätverket en 128-bits anrop till användarens mobil. SIM-kortet i mobilen använder A3 algoritmen och Individual Subscriber Authentication Key(Ki, unik för varje SIM) för att beräkna Signed RESponse(SRES) och skicka tillbaka till basstationen. Om SRES matchar för beräkningens värde i basstationen sker följande.

Här använder SIM olika algoritmer, A8, Ki och det original anropet för att beräkna Session Key (Kc) och skickar detta till basstationen. Session Key användes enskilt med A5 algoritmen för att kryptera data som skicka över radioöverföring (Figur 2).



Figur 2: GSM användare autentisering.

3.3 Algoritmen

A3 och A8 algoritmen implementeras i SIM kortet som oftast används tillsammans som en algoritm (A38) för beräkna SRES och Kc parallellt. Dessa två algoritmen använder COMP-128 som är stark hash funktion. Det tar 128 bitars anrop, 128 bitars Ki som ingång och ut ett 128-bitar värde, som delas i, 32 bitar av anrop, 32 bitar för SRES och 64 bitar för Kc. Den här algoritmen visas att man kan knäckas inom 8 timmar, och specifikationen för COMP-128 är redan tillgängligt på Internet. Det har lett till att två versioner av COMP-128 tagits fram.

A5 algoritmen är en ström chiffer. Det har blivit implementerad mycket effektivt i hårdvaran och designen har aldrig gjorts offentlig. Det är tre olika versioner av A5: A5/1 som är en stark version, A5/2 som är en svag version och A5/3 som är baserad på algoritmerna som används i 3G telefoner. Det finns även A5/0 men den har ingen kryptering.
Dessa algoritmerna kan även knäckas ganska enkelt. Genom att skanna utgången av A5/1 i 2 minuter så tar det mindre än två sekunder att knäcka. Den svaga A5/2 algoritmen kan knäckas inom millisekunder och attack mot A5/3 genom att använda krypterings skanning av A5/1.

3.4 Utrustningssäkerhet

IMSI (International Mobile Subscriber Identity) är en unik identitet för varje GSM-telefonabonnent. Identiteten är knuten till SIM-kortet och IMSI finns beskrivet i ETSI GSM standard. EIR har en klassificering för varje IMEI nummer, Vit: giltig telefon, Grå: telefoner som spåras och Svart: spärrad telefon (borttappad eller stulen).

3.5 Säkerhet för användaren

Individer kan vara identifierade genom International Mobile Subscriber Identity på deras SIM kort. För att förhindra personer att lyssna på det, skickas en temporär IMSI när man kommunicerar med basstationen, när telefonen slås på eller när ett samtal påbörjas.

4 UMTS

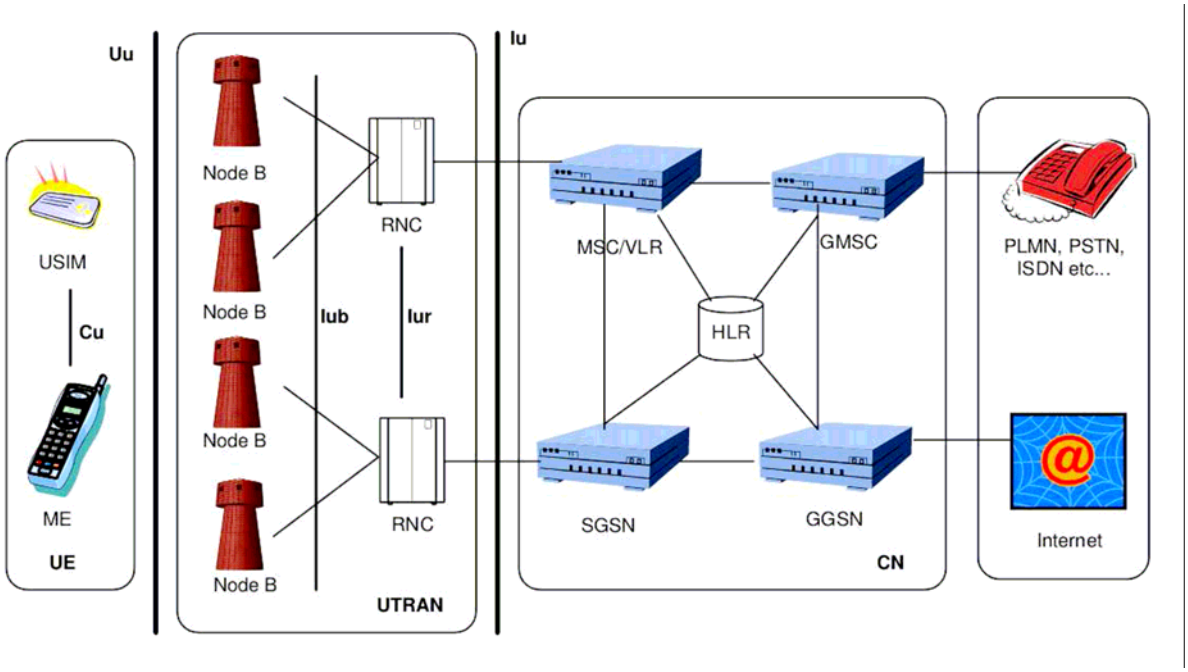
UMTS *Universal Mobile Telecommunications System*, är tredje generationens Mobiltelefonisystem som definierad av European Telecommunications Standards Institute (ETSI) och som innebär bredbandig, datapaketbaserad överföring av text, bilder, röst, video och multimedia med överföringshastigheten upp till 2 megabit per sekund. Detta ökar kraven på säkerheten för att inte tillåta möjligheten att angripa 3G mobilenhet. UMTS teknologin är baserad på GSM (Global System for Mobile) kommunikations standard. Men förbättringar har gjorts i visa delar och även skapat nya funktioner för att öka säkerheten. I det här kapitlet presenteras arkitekturen och säkerhetsmekanism inom UMTS. Post- och telestyrelsen, PTS, är den myndighet som har fördelat UMTS tillstånden i Sverige.

4.1 System översikt

Strukturen över UMTS nät är baserad på GSM:s nät. Förbättringar har gjorts och ny teknik har lagts till beroende på tjänster som 3G erbjuder. Figur 3, ger en överblick över nätet.

- *User Equipment (UE)* – UE består av Mobile Equipment(ME) en mobil och en USIM (*User Services Identity Module)*. USIM är ett smart kort som håller reda på abonnentens identitet, autentiserings algoritmer och som dessutom lagrar olika nycklar för säkerheten. User Equipment är ekvivalent med Mobile Station i GSM och kommer att refereras som Mobile Station(MS) i avsnitten nedan.
- *Node B* – är ekvivalent med Base Station (BTS) i GSM. Dess uppgift är att omvandla dataflödet över Uu och lu gränssnittet
- *Radio Network Controller (RNC)* – är ekvivalent med BSC (Base Station Controller) i GSM. Den kontrollerar sändningsresurserna i en domän av B noder som är ansluten till RNC.
- *Mobile Switching Center / Visitor Location Register (MSC/VLR)* – MCS fungerar som en switch, och databasen (VLR) skickar MS (Mobile Station) med dess nuvarande läge för *Circuit Switched (CS)* tjänsten.
- *Gateway Mobile Switching Center (GMSC)* – behandlar all krets kopplad (CS) kommunikation mellan UMTS nätverk och externa CS nätverk.

- *Serving GPRS Support Node (SGSN)* – SGSN beter sig som MCS/VLR men används typiskt för paketförmedlande (PS) tjänsten.
- *Gateway GPRS Support Node (GGSN)* – GGSN tillämpar nästan samma funktionalitet som Paket tjänsten så som GMSC gör för Circuit Switched domän.
- *Home Location Register (HLR)* – HLR lagrar abonnentens specifika data. När en UMTS-operator delar ut ett SIM kort till abonnenter, då lagrar operatorn en kopia av det väsentliga av SIM kortets information (Ki och IMSI) det är HLR. Ki behålls hemligt för andra operatörer.



Figur 3: UMTS Arkitektur.

4.2 Säkerhetsaspekter

Säkerheten i 3G arkitekturen utnyttjar en del av det användbara av 2G:s säkerhetslösningar, och försöker att återgärda de buggar som har upptäckts i 2G. I 3G introduceras även nya aspekter som kommer att skydda de nya tjänsterna i 3G.

4.2.1 Bibehållna säkerhetsaspekter i 2G

3GPP har beslutat att behålla (och utveckla) vissa säkerhetselement av 2G. Se följande exempel.

-

Abonnent Autentisering

Det existerar en oföränderlig hemlig nyckel Ki för varje användare *i*. Figur 4 nedan förklarar att nyckeln är lagrad i två platser.

1. i användarens *Subscriber Identity Module* (SIM) kort.
2. på Authentication Center (AuC).

Nyckeln Ki lämnar aldrig de här två platserna.

- Kryptering av kommunikationen över radiogränssnitt.

  Under autentiseringen etableras en hemlig sessions nyckel Kc. Med den här nyckeln krypteras alla samtal mellan telefonen och basstationen tills nästa autentisering inträffar. Krypteringsalgoritmen heter A5, figur 5 nedan förklarar på hög nivå strukturen för GSM:s krypteringsalgoritm A5.

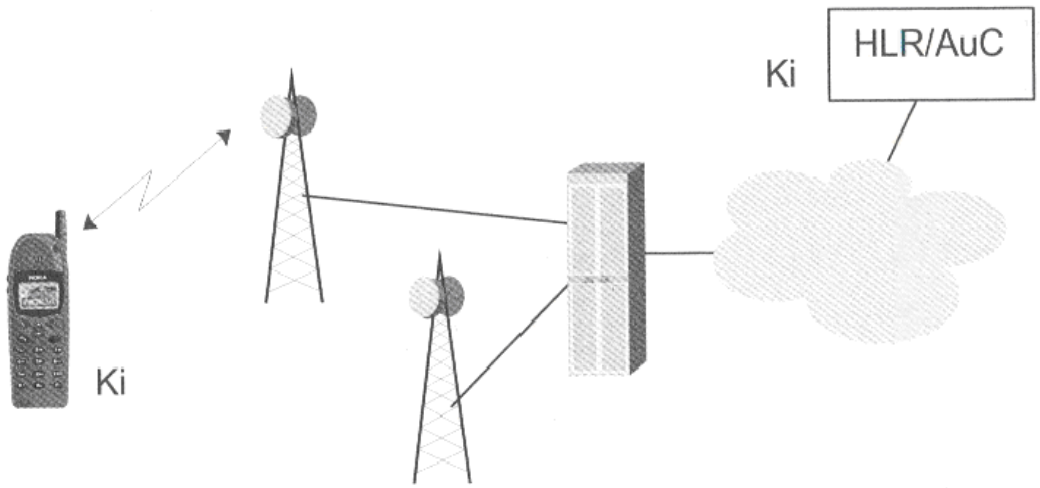
- Förtroende avseende abonnentens identitet över radiogränssnitt.

  Den permanenta identiteten för användaren—International Mobile Subscriber Identity (IMSI)—är skyddad i GSM mot tjuvlyssnare genom att begränsa antalet situationer när det behövs användas. Istället för IMSI, Temporary Mobile Subscriber Identity (TMSI) används normalt för identifiera användaren. TMSI ändras ständigt varje gång det har använts och en ny TMSI överförs alltid till användaren över krypteringskanalen. En liknande mekanism användes i UMTS.

4.2.2 Brister i GSM:s säkerhet

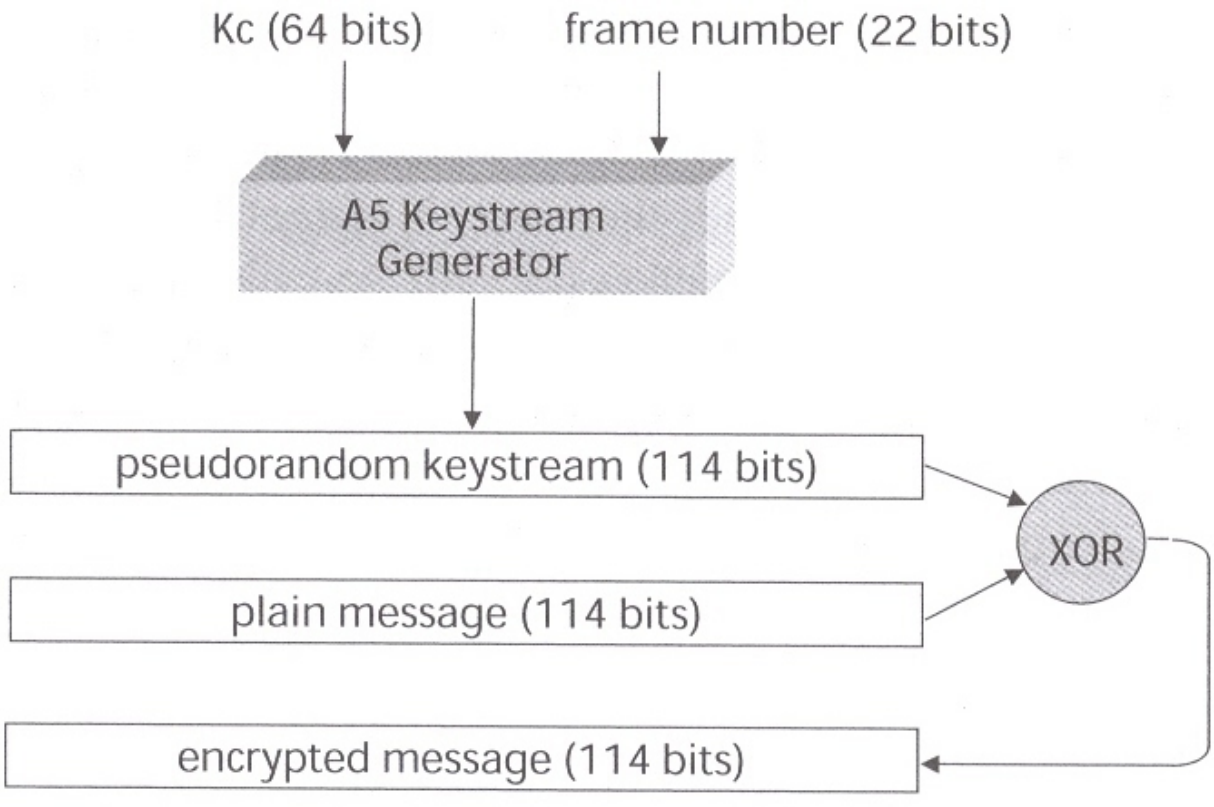
Följande brister som finns i 2G är korrigerande i 3G.

- Aktiva attacker genom att utnyttja falsk BTS (Node B i UMTS).
- Nyckelchiffrering och autentisering av dataöverföring mellan och inuti nätverken.
- Kryptering är inte tillräckligt i längden. Överföring av klartext av användaren och datasignaler över mikrovågsförbindelse (i GSM, från BTS till BSC).
- Ingen dataintegritet är förutsatt.
- 2G systemet innehåller ingen god flexibilitet för uppgradering.
- Nätverket i 2G systemet har ingen kännedom eller kontroll över hur nätverkstjänsten utnyttjar autentiseringsparametrar för abonnenten.



GSM = Global System for Mobile communications; HLR = Home Location Register; AuC = Authentication Centre

Figur 4: Abonnentautentisering



Figur 5: Strukturen för A5 strömchiffer.

4.3 Säkerhetsarkitektur

Det finns fem säkerhetsskillnader i 3G. Förklaring för alla fem kommer att tas upp i avsnitt nedan.

- **Network access security** – Skyddar från otillåten access till nätet och de tjänster som erbjuds.
- **Network domain security –** Erbjuder säkerhet när data överförs från en domän till en annan.
- **User domain security** – Erbjuder säkerhet i överföringen mellan användare och basstation.
- **Application domain security** – Sköter säkerheten mellan applikationer som utbyter data mellan domäner.
- **Visibility and configurability of security** – Informerar användaren om vilken typ av säkerhet som för närvarande används samt den säkerhetsnivå som rekommenderas för en viss typ av tjänst

4.3.1 Network access security

4.3.1.1 User identity confidentiality

Abonnentens identitet i UMTS är (IMSI**)** International Mobile Subscriber Identity (samma fall är i GSM). Identifiering av abonnenter i UTRAN (UMTS Terrestrial Radio Access Network) är i alla fall betydelsen av temporär identitet: TMSI i CS domänen eller P-TMSI i PS domänen. Förtroendet för abonnentens identitet är därför skyddad (nästan alltid) mot passiv tjuvlyssning.

4.3.1.2 Authentication of users

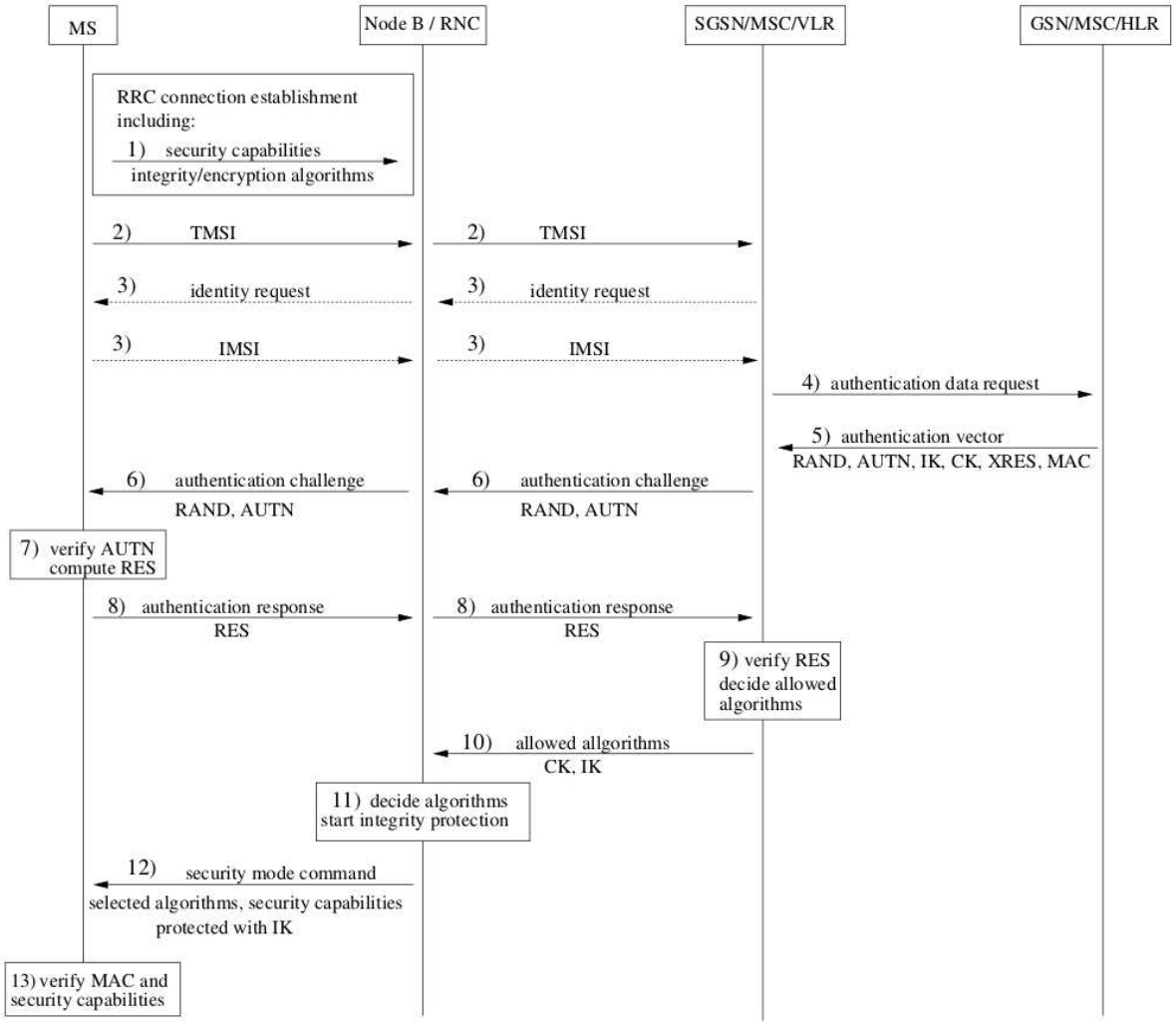
Metoden som används I UMTS för *Authentication and Key Agreement (AKA)* (se figur 6). Mekanismen var från början designad genom att kombinera två olika autentiserings mekanismer, GSM:s Authentication and Key Agreement mekanism och den generella autentiseringsmekanismen baserad på sekvens nummer (SEQ). SEQ finns i USIM och Home Environment(HE) och står för gemensam autentisering mellan User Equiment och nätverket (se figur 7). Nyklarna i UMTS skyddas av funktionerna f1-f5 (se figur 7) där alla är av envägstyp och är baserade på samma algoritm. Grundprinciper av algoritmerna gör det omöjligt att härleda information om utgången av en funktion genom att känna till utgången från de andra funktionerna.

4.3.1.3 User data confidentiality

Mekanismen för att skydda datakonfidentialitet för användarens information och dataöverföring i UMTS kräver en krypteringsfunktion f8. Krypteringen liknar metoden som används i GSM men förbättringar har gjorts för UMTS. Krypteringen skyddar endast data som skickas över radioaccessförbindelsen mellan User Equipment (UE) och Radio Network Controller (RNC). Därför har krypteringen implementerats i UE och i RNC. F8 är ett symmetriskt synkroniserat strömchiffer med en 128-bitars hemlig krypteringsnyckel CK. F8 används för att kryptera klartext genom att applicera en keystream med bitvis XOR operation. Klartexten kan återställas genom att generera samma nyckelström med samma ingångsparameter och applicera klartexten med bitvis XOR-operation. COUNT är 32 bitar, BEARER är 5 bitar och DIRECTION är 1 bits (se figur 8). F8 är baserad på Kasumi algoritmen.

4.3.1.4 Data integrity

Radiogränssnittet i 3G mobilsystemet har även byggts för att stödja integritetsskydd på överföringskanalen. Det möjliggör för mottagandeidentiteten att verifieras, så att dataöverföringen inte har modifierats på ett obehörigt sätt sedan det har skickats. Dessutom garanteras att den ursprungliga dataöverföringen kräver en gångs avhämtning. Mekanismen för integritetssäkerhet är avsedd för användaren på grund av prestation anländning. Funktionen f9 används endast för autentisera integriteten och ursprungligen för datasignaler mellan MS och RNC i UMTS. F9 beräknar 32 bitars Message Authentication Code (MAC), som är visad i bilden och kontrolleras av mottagaren. Huvudingångarna till algoritmen är av 128 bitars hemlig integritetsnyckel IK, och variabellängden innehåller meddelande. COUNT är 32 bitar, FRESH är 32 bitar och DIRECTION är 1-bit (se figure 9). F9 är också baserad på är Kasumi algoritmen.



Figur 6: UMTS Authentication and Key Agreement

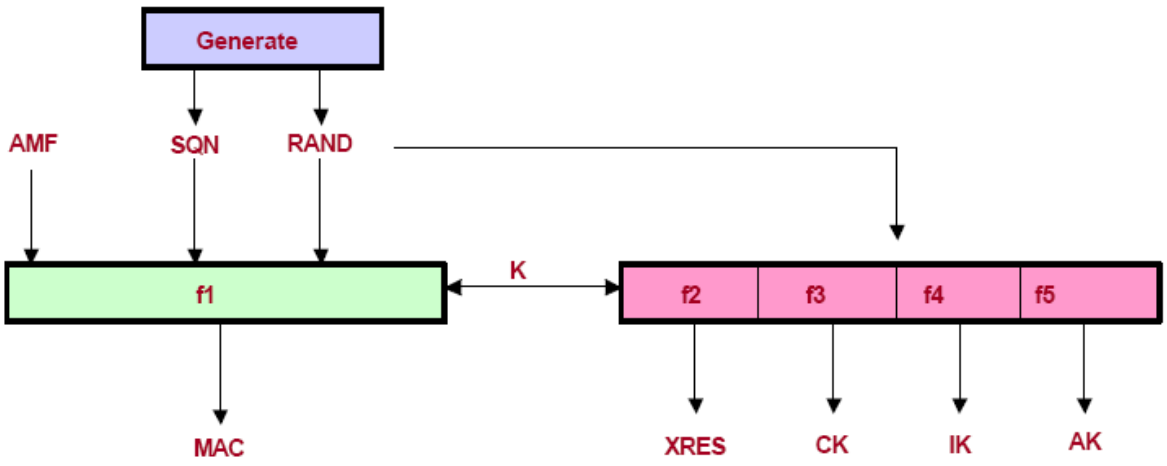


Figure 7: Generating av autentiseringsvektor i AuC.

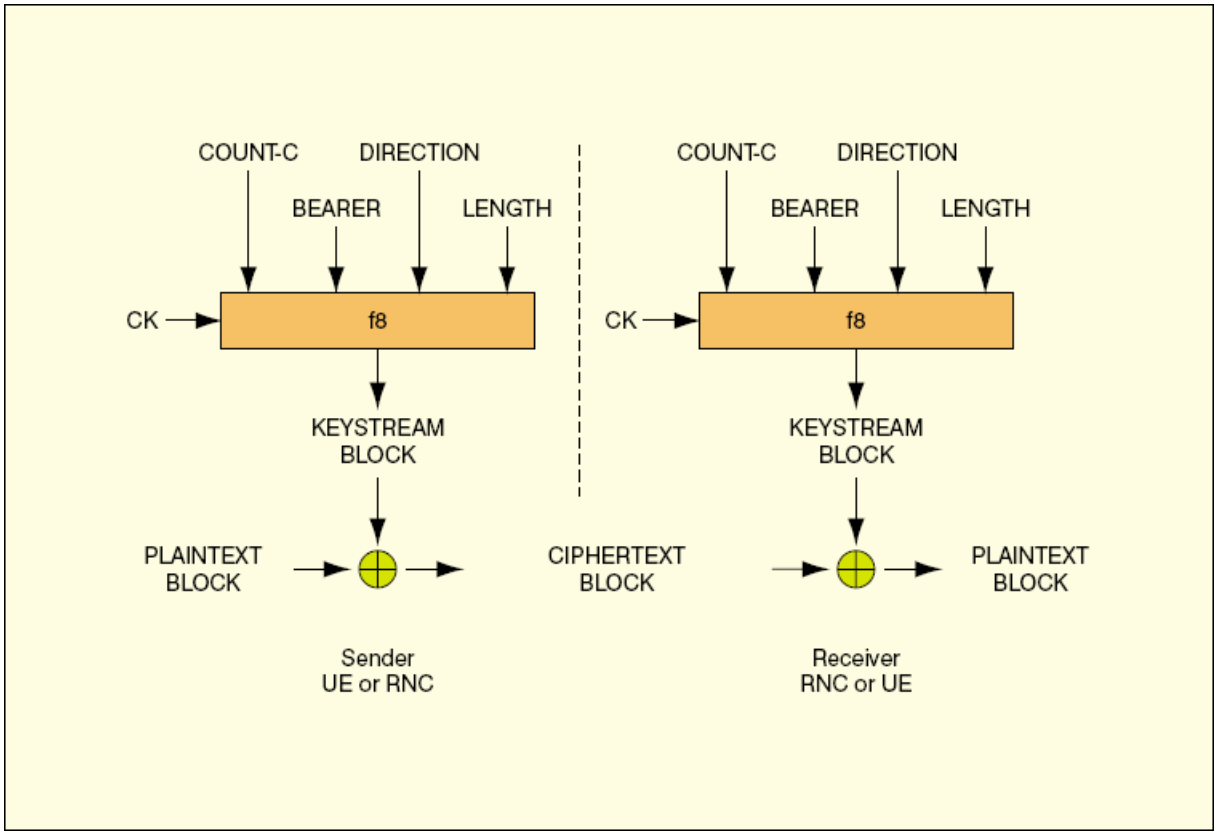


Figure 8: Chifferalgoritmen F8 mellan RNC och UE/MS

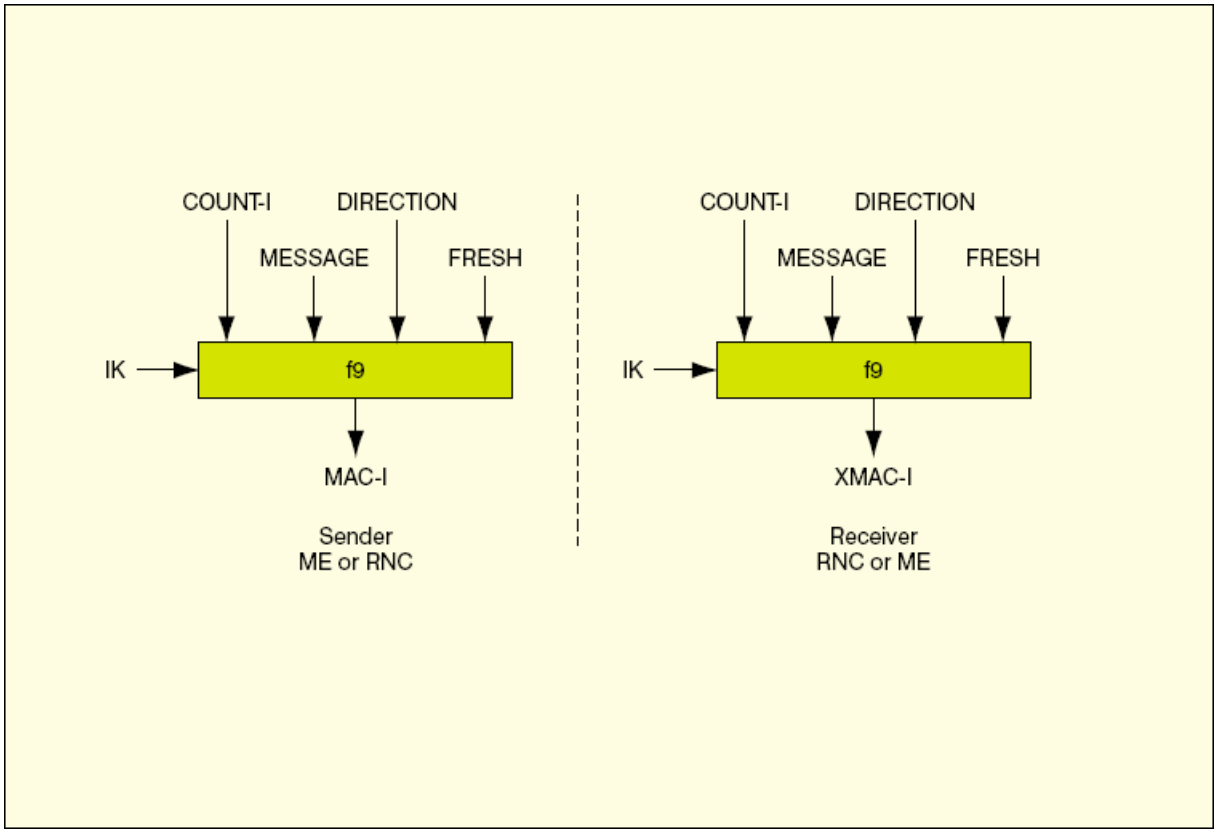


Figure 9: Beräkning av MAC ur meddelandet

4.3.2 Network Domain Security

Termen ‘network domain security’ i 3G motsvarar säkerheten för kommunikationen mellan nätverkselement. I detta fall så har User Equipment (UE) ingen påverkan på network domain security. Två kommunicerande nätverkselement kan tillhöra samma administrerade nätverk med en User Equipment (UE) eller kan de tillhöra två olika nätverk. Mobile Application Part (MAP) är ett protokoll som har hand om säkerheten mellan mobilen och stationen. För att skydda all kommunikation i nätverket är det inte tillräckligt att skydda bara MAP protokollet. Från mobil kommunikationssynvinkel, så är MAP nödvändigt del att skydda. Som exempel kan nämnas, sessionsnycklar som skyddar radiogränssnittet och annan dataautentisering som behandlas i MAP.

Observera att 3GPP har specificerat hur MAP protokollet kan köras ovanpå IP. I det här fallet är det två grundmetoder att välja mellan för att skydda MAP, MAPsec eller IPsec. Fördelen är att skyddet täcker lägre lager i headern så som har gjorts i IP nivån. Säkerheten som är baserad på SS7[1] protokollen skall utföras på applikationsnivå.

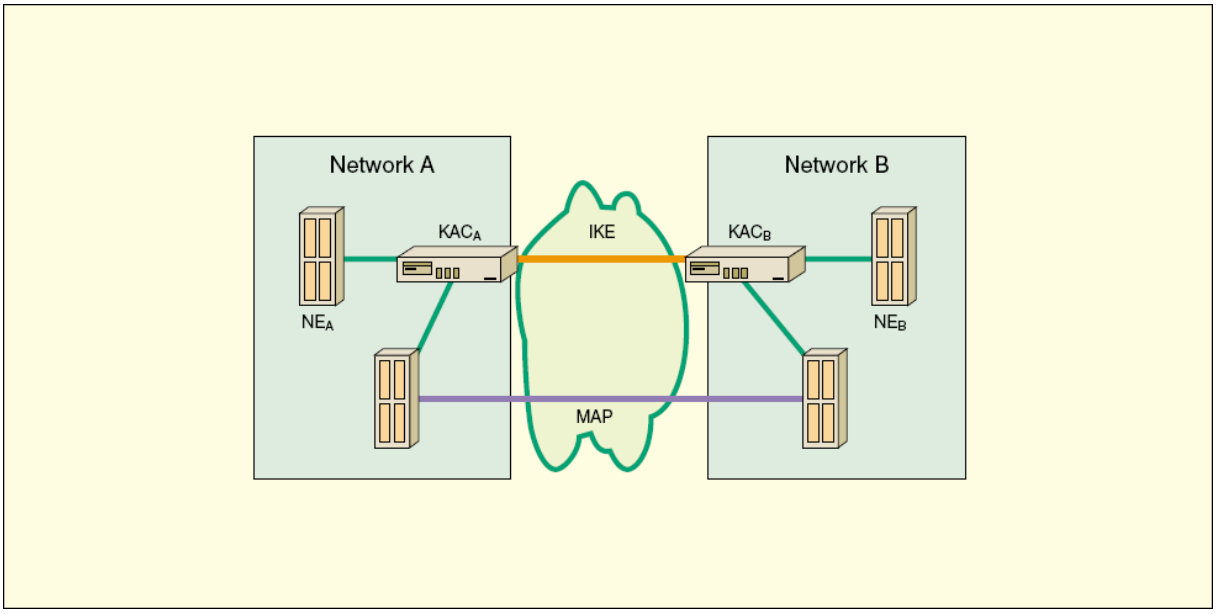
4.3.2.1 MAPsec

Den huvudsakliga idén bakom MAPsec kan beskrivas enligt följande. Ett MAP-meddelande i form av klartext krypteras och resultatet placeras i en bägare inåt i ett annat MAP-meddelande. Samtidigt så skyddar en kryptografisk checksumma (tex en Message Authentication Code(MAC)) det ursprungliga meddelandet som inkluderar det nya MAP-meddelandet. Nycklar behövs för att kunna använda krypteringen och MAC:s (se figur 10).

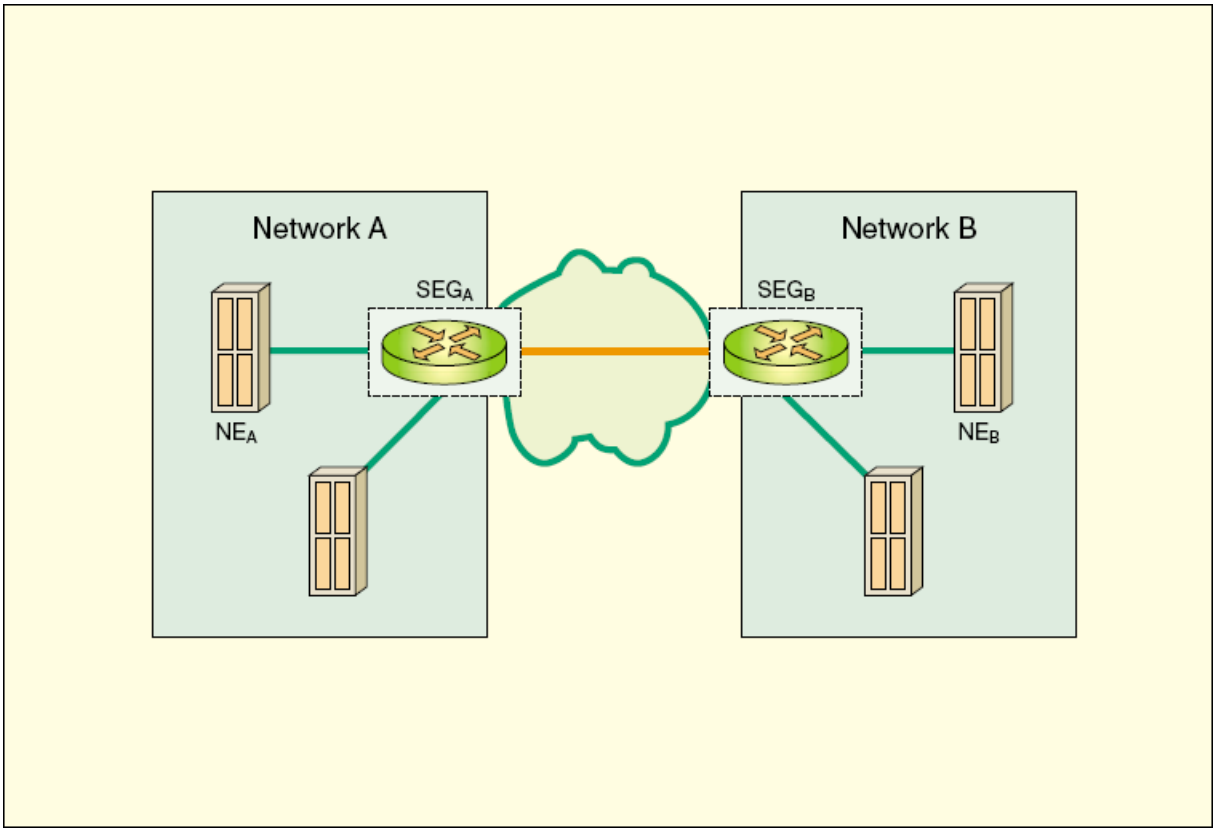
4.3.2.2 IPsec

I IPsec så styrs kommunikationen på IP nivån genom de externa nätverken som måste gå via ett nytt element som heter säkerhetsgateway(SEG) (se figur 11). Dessa gateways använder IKE-protokollet för att utbyta IPsec:s SA:s mellan sig själva. En viktig begreppsmässig skillnad mellan säkerhetsgateway och MAPsec:s KAC är att den förra utnyttjar även själv SA:s, medan den senare distribuerar till andra element, vilka skickar och tar emot de faktiska MAPsec-meddelandena.

([1]SS7 är internationellt telekommunikationsprotokoll för överföring av digital data över bredbandsnätverk).



Figur 10: Användning av MAPsec.



Figur 11: Användning av IPsec.

4.3.3 User Domain Security

Personal identification number (PIN) är en funktion som finns i GSM systemet och som har behållits i UMTS systemet, PIN är en kod som endast användaren(UE) och USIM känner till. USIM representerar och identifierar användaren och hans/hennes förknippning till ME. Kortet har ansvar för att framföra användaren och nätverksautentisering. Även en säkerhetskod som användaren är tvungen att ange (ett PIN) som kan vara 4-7 siffror lång kod till USIM för att han/hon skall få access till 3G tjänsten. För att man inte skall kunna förfalska ett SIMkort så har säkerheten delats mellan USIM och terminalen. Om ett USIM misslyckas med att bevisa säkerheten då misslyckas accessen till terminalen. Kortet kan tänkas innehålla användarens profil.

4.3.4 Application Domain Security

Application domain security säkrar informationen mellan UE och leverantören över nätverket med säkerhetsnivå som väljs av operatören eller leverantören. En otillgänglig applikation skall autentisera användaren innan han får tillåtelse för att utnyttja tjänsten, och kan även vara försedd med en applikationsnivå för datakonfidentialitet. Säkerhetsmekanismen för applikationsnivån behövs för att funktionaliteten i de lägre nivåer kan inte garantera säkerhetsvillkor hela vägen ut.

4.3.5 Security visibility and Configurability

Ett synligt kännetecken skall informera användaren när kryptering används och när användaren förflyttar sig från 3G till 2G täckning som en slutlig mekanism för att upptäcka möjlig attack. Det här kan inkluderas, (a) indikation av kryptering för nätverksaccess, (b) indikation av kryptering på själva nätverket, (c) indikation av säkerhets nivå (tex när en användare förflyttar sig från 3G till 2G). Konfigurationen möjliggör för användaren och HE att konfigurera om åtgärden av tjänsten är beroende på aktivering av säkerhetsattribut. En tjänst kan endast utnyttjas när alla relevanta säkerhetsattribut är aktiva. Konfigurationsattributen som föreslagits inkluderar, (a) aktivera/inaktivera användarens USIM autentisering för säker tjänst, (b) acceptera/hindra inkommande okrypterade samtal, (c) acceptera/hindra användning av säker krypteringsalgoritmer.

5 3G Standard

ITU har godkänt globala rekommendationer för tredje generationens mobilsystem under beteckningen IMT-2000, som har standardiserats av regionala standardiseringsorgan. IMT-2000 rymmer fem varianter och Europa använder två av dem, WCDMA och TD-CDMA, i Europa även kallat UMTS

5.1 WCDMA

UMTS-systemet baseras på WCDMA som är en radioaccessteknik. WCDMA skall stödja mediatjänster som t.ex. vanlig telefoni, multimediatjänster och videotelefoni. WCDMA utnyttjar höga datahastigheter från 384 kbps i alla radiomiljöer och ända upp till 2 Mbps i mobila miljöer med låg hastighet och inomhusmiljöer. WCDMA är en väldigt flexibel service, varje 5 MHz bärvåg klarar av att hantera blandade servicetjänster med hastigheter från 8 kbps upp till 2 Mbps.

I UMTS så finns det två variationer av WCDMA teknologin. Frequency division duplex(FDD). Skillnaden är hur uplink och downlink separeras från varandra. I FDD så utnyttjas uplink frekvenser mellan 1,920MHz – 1,980MHz medan downlink utnyttjar frekvenser mellan 2,110MHz – 2,170MHz. I Time division duplex (TDD) så utnyttjar både uplink och downlink samma frekvenser men olika tidsintervall. Det finns två frekvensband som utnyttjas av olika TDD-varianter. Dessa frekvensband ligger mellan 1,900MHz – 1,920MHz och 1,980MHz – 1,995MHz. Länken delas in i rutor (frames) där varje ruta är 10ms och innehåller 16 luckor (slots) som är 0.625 ms vardera. I regel avses downlink som länken från basstationer till mobilenheter och uplink som från mobil till basstation.

5.2 CDMA2000

Standaren CDMA2000 tillhör familjen av 3G mobil telekommunikation som använder CDMA, ett multipelt accesssystem för digital radio, för att skicka röst, data, datasignaler (såsom en uppringt telefonnummer) mellan mobiltelefonen och telefonmasten. Det är andra generationen av CDMA digital telefoni.

CDMA (code division multiple access) är en mobil digital radioteknologi som överför strömmar av bitar och vars kanaler divideras med en kod (PN sekvens). CDMA tillåter många radiosignaler att dela samma frekvenskanal. TDMA (time division multiple access) som används i GSM skiljs från CDMA, tekniken är annorlunda, alla signaler kan vara aktiverade hela tiden, eftersom nätverkskapaciteten inte direkt begränsar antalet aktiva signaler. Eftersom en mängd av telefoner kan betjänas av några telefonmaster, har CDMA standaren en

signifikant ekonomisk fördel över TDMA standaren, eller den gamla cellulär standaren som använde frequency division multiple access (FDMA).

5.3 TD-CDMA

TD-CDMA är ett primärt radio gränssnitt som används av UMTS-TDD. UMTS-TDD är en mobil nätverksstandard som bygger på 3G cellulär mobiltelefonsstandard, vilken använder TD-CDMA och TD-SCDMA. TD-CDMA använder 5MHz tillväxt av spektrum, alla luckor(slots) divideras i 10ms ramar(frames) som rymmer femton tidsluckor (1500 per sekund). Tidsluckorna är lokaliserade i bestämd del för downlink och uplink. Code Division Multiple Access(CDMA) används inom varje tidslucka för att multiplexa strömmar från och till multiple transceivers.

Ett alternativ av radio gränssnitt för UMTS-TDD är TD-SCDMA, som använder 1,6MHz bitar av spektrum, och är standardiserad i UMTS.

5.4 TD-SCDMA

Time Division-Synchronous Code Division Multiple Access är en 3G mobil telekommunikations standard.
TD-SCDMA använder TDD, jämfört med FDD system som används av WCDMA. Genom att använda dynamiskt antal tidsluckor för downlink och uplink, kan systemet lättare anpassa asymmetrisk trafik med dataskillnaden av värdets behov på downlink och uplink än FDD systemet. Eftersom det inte behövs parvis spektrum för downlink och uplink, ökas flexibiliteten när det gäller placering av spektrum. Användning av samma frekvensbärare för downlink och uplink, betyder att kanalvillkoren är samma för båda riktningarna och basstationen kan ansluta sig till downlinks kanalsinformationen från uplinks kanaluppskattning, som är utgör ett stödd applikationen för vågledar teknologin.

5.5 EDGE eller EGPRS

Datahastighets förbättring för GSM utveckling (EDGE) eller förbättring av GPRS (EGPRS), är digital mobiltelefoni teknologi detta ta hänsyn till ökad dataöverföringshastighet och en förbättring för dataöverföringens tillförlitlighet. Det är allmänt klassificerad för 2.75G nätverkteknologi. EDGE har införts i GSM nätverken runt hela värden sedan 2003 och i början i Nord Amerika. Det kan användas för varje paketförmedlarapplikation som Internet kommunikation. Hög-hastighets dataapplikationer som videotjänster och andra multimedia utnyttjar fördelarna med EGPRS som har förstärkt datakapacitet.

6 UMTS Svagheter

6.1 IMSI kan skickas som klartext

Användarens mobila identitet och lokalisering är värdefull information som behöver skyddas. En möjlig svaghet i 3G säkerhets arkitektur är en backupprocedur för TMSI verkliga läge. Speciellt när SN/VLR inte kan förbinda TMSI med International Mobile Subscribers Identity (IMSI) eftersom TMSI kan skadas eller databas brist, VLR skall begära att användaren identifieriar sig själv med hjälp av IMSI vi radio. Dessutom när användaren vandrar omkring och SN/VLR inte kan etablera förbindelse med föregående VLR:er, eller inte kan återställa användarens identitet. SN/VLR skall också begära att användaren identifierar sig själv via radioförbindelse**.** Det kan leda till att en aktiv attack där inkräktaren låtsas vara en ny SN för vilken användaren avslöjar sin verkliga identitet. I båda fallen, så är IMSI den som representerar den verkliga användarens identitet, som överförs som klartext över radiogränssnittet där användarens konfidentialitet kränks.

6.2 Intern säkerhet

UMTS ryggrad är skyddad av Network Domain Security (NDS). Det säkerheten är inte tillräckligt mot attacker som uppstår från elaka abonnenter och nätverks operatörs personal. En överdebiteringsattack är svårare att starta med integritets skydd av meddelande överföring i UMTS, med samma typer av attack där en abonnent attackerar en annan kan vara möjligt. Brandväggar erbjuder begränsad säkerhet genom mobilen liksom brandväggen som inte kan skilja mellan tjänster och tillåter direkt anslutning.

6.3 Möjlig samverkning med GSM

Om abonnenten går utanför 3G täckning, då används GSM istället. Detta kan äventyra säkerheten. UMTS abonnenten kan lida för Man I Mitten attack i en hybrid GSM/UMTS miljö.

7 3G attacker

Under den rubriken kommer dem olika typer av attacker att förklaras. Här används engelska rubriker på grund av att den svenska översättningen inte kommer att tillräckligt överensstämma med det engelska. Fetstil och kursiverade rubriker anses vara de attacker som är viktigast och har förklarats noggrant, resten har förklarats kortfattat.

7.1 Översikt inom attacker

- **Tjuvlyssna (Eavesdropping)** - Inkräktare knyter sig till andra användare för att tjuvlyssna på deras samtal och även data förbindelsen. Metoden för att kunna lyckas är att modifiera MS.

- **Förfalskning av användaren (Impersonation of a user)** - Inkräktaren använder sin skicklighet genom att skicka användarens kommunikation eller data till nätverket, genom att försöka tvinga nätverket att tro att informationen kommer från verkliga användaren. Metoden för att kunna lyckas är även att modifiera MS.

- **Förfalskning av nätverket (Impersonation of the network)** - Inkräktaren använder sin skicklighet genom att skicka användarens kommunikation eller data till ett offer, genom att försöka tvinga nätverket att tro att information kommer från verkliga nätverket. Metoden för att kunna lyckas är att modifiera BS.

- **Man i mitten (Man-in-the-middle)** - En Man-in-the-Middle (MITM) attack är en attack som har förmåga att läsa, införa och modifiera efter behov. Den obehöriga kopplar in sig på en förbindelse i smyg och uppfångar meddelanden mellan A och B. A och B tror alltså att de skriver direkt till varandra, men i själva verket kommunicerar båda med en tredje person. Metoden för att kunna lyckas är att modifiera BS med anslutning till MS.

- **Kompromettera autentiseringsvektor i nätet (Compromising authentication vectors in the network)** - Inkräktaren tar kontroll av kompromettерade autentiseringsvektorer i nätet, som kan inkludera anrop/svar, chiffer nycklar och integritetsnycklar. Dessa data kan erhålla genom att kompromettera nätets noder eller genom att hindra överföring av meddelanden på nätets länk. Metoden för att kunna lyckas är att modifiera MS eller att modifiera BS.

7.2 Denial of service

Här diskuteras följande denial of service attacker:

7.2.1 *User de-registration reguest spoofing*

En attack som kräver modifiering av MS och utnyttjar svagheten att meddelanden inte kan autentiseras av nätverket när de tas emot över radiogränssnittet. Inkräktaren förfalskar en avregistreringsbegäran (IMSI detach) till nätverket. Nätverket avregistrerar användaren från det besökta området och instruerar HLR för att utföra samma sak. Därefter är användaren oåtkomlig för mobil terminal service.

Hindrar 3G:s säkerhetsarkitektur attacken: JA.

Integritetsskydd av kritiska meddelanden skyddar mot attacken. Mer specifikt, data autentiseras och hindrar alltid upprepning av avregistreringsbegäran från det betjänande nätverket för att verifiera att avregistreringsbegäran är legitimerad.

7.2.2 Location update reguest spoofing

Istället för att skicka begäran för avregistrering, skickas attacken en lokaliserings-uppdateringsbegäran från ett annat område än den användaren som för närvarande är registrerad i. Detta resulterar att användaren registreras i ett nytt område.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

7.2.3 *Camping on a false BS*

En attack som kräver modifiering av BS och utnyttjar svagheten att användaren kan bli lockad till en falsk basstation. När användaren är ansluten till en kanal på en falsk basstation, då är användaren utom räckhåll för nätverks sökning för att bli registrerad.

Hindrar 3G:s säkerhetsarkitektur attacken: NEJ.

Säkerhets arkitektur hindrar inte den typen av attack. Hur som helst, denial of service i detta fall varar så länge attacken är aktiv till skillnad från attacken ovan där denial of service även varar efter det att själva attacken har avslutar. Dessa attacker är jämförbara med radiostörning vilket är mycket svårt att effektivt hindra i något radiosystem.

7.2.4 Camping on a false BS/MS

En attack som kräver modifiering av BS/MS och utnyttjar svagheten att användaren kan bli lockad till en falsk basstation. En falsk BS/MS kan fungera som repeater

ibland och kan förmedla förfrågningar mellan nätverket och användaren, men därefter modifierar eller ignorerar vissa förfrågningar relaterade till användaren.

Hindrar 3G:s säkerhetsarkitektur attacken: NEJ

7.3 Identity catching

Här identifiera följande typer av attacker mot användarens konfidentialitet:

7.3.1 *Passive identity catching*

En passiv attack som kräver modifiering av MS och utnyttjar svagheten att nätverket ibland kan begära att användaren skickar sin identitet i klartext.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

Mekanismen för identitets konfidentialitet hindrar sådana attacker. Användning av temporär identitetslokalisering genom nätverken gör passiv tjuvlyssning ineffektiv eftersom användaren måste avvakta en ny registrering eller dålig matchning i nätverkets databas innan han kan griper användarens fasta identitet i klartext. Det ineffektiva i denna attack ger troligtvis belöning till attackeraren som göra att det tänkta utfallet osannolikt.

7.3.2 Active identity catching

En aktiv attack som kräver modifiering av BS och utnyttjar svagheten så att nätverket ibland kan begära att MS skickar användarens permanenta identitet i klartext. Attackeraren med en modifierad BS lockar användaren att lägga användaren på hans BS och sedan blir han frågad för att skicka sin International Mobile Subscriber Identity (IMSI).

Hindrar 3G:s säkerhetsarkitektur attacken: JA

7.4 Impersonation of the network

Här identifieras följande attacker där inkräktaren imiterar det verkliga nätverket. Målet av sådana attacker är oftast att tjuvlyssna på användarens data eller att skicka användarens information som han därefter tror härrör från det verkliga nätverket eller användaren till vilken han är ansluten via nätverket.

7.4.1 Impersonation of the network by suppressing encryption between the target user and the intruder

En attack som kräver modifiering av BS och utnyttjar svagheten att meddelanden inte autentiseras av MS när de tas emot över radiogränssnittet. Attackeraren med en

modifierad BS lockar användaren in på den falska BS och när tjänsten väl är initierad, då omöjliggörs krypteringen av inkräktaren.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

7.4.2 *Impersonation of the network by suppressing encryption between the target user and the true network*

En attack som kräver modifiering av BS/MS och utnyttjar svagheten av att meddelanden inte autentiseras av nätverket när de tas emot över radiogränssnittet. Användaren lockas på den falska BS/MS. När ett samtal sätts igång, modifierar den falska BS/MS krypteringsmöjligheterna för MS för att det ska verka som om get finns en inkompatibilitet mellan nätverket och mobilen. Nätverket kan sedan besluta att upprätta en okrypterad förbindelse. Efter beslutet har tagits att inte använda kryptering, avbryter inkräktaren kommunikationen med nätverket och förfalskar nätverket till användaren.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

Ett mobilstationskommando med meddelandeautentisering och upprepningshinder tillåter nätverket att verifiera krypteringen som inte blivit avstängd av inkräktaren.

7.4.3 *Impersonation of the network by forcing the use of a compromised cipher key*

En attack som kräver modifiering av BS/MS och att inkräktaren förfogar över en falsk autentiseringsvektor och därför utnyttjas svagheten att användaren inte har kontroll över krypteringsnyckeln. Användaren lockas in på den falska BS/MS. När ett samtal sättas igång, tvingar den falska BS/MS användaren att identifiera krypterings nyckel på användarens mobil. Inkräktaren uppehåller samtalet så länge det behövs eller så länge angreppet inte upptäcks.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

användandet av sekvensnummer i anropet tillåter USIM att verifiera färskheten av krypteringsnyckeln för att skydda mot återanvändning av den falska autentiseringsvektorn. Men arkitekturen ger inte skydd mot tvingad användning av förfalskad autentiseringsvektor som ännu inte har använts för att autentisera USIM. Därför är dessa nätverk fortfarande sårbara för attacker som utnyttjar sig av förfalskade autentiseringsvektorer vilket har avbrutits mellan skapandet i autentiseringscentret och användning i nätverket.
Användaren måste kunna lita på SN för att med säkerhet kunna behandla autentiseringsvektorn. Exempelvis, kan en inkräktare med en falsk BS tränga sig in hemligt med en SN för att få tag på en oanvänd autentiseringsvektor, eller kan SN

utsätta sig själv för onödig risk för att lagra ett stort antal autentiseringsvektorer innan de behöver användas.

7.5 Eavesdropping on user data

Här identifieras följande attacker med syftet att tjuvlyssna på användarens data vilken överförs genom det verkliga nätverket till avsedd mottagare:

7.5.1 *Eavesdropping on user data by suppressing encryption between the target user and the intruder*

En attack som kräver modifiering av BS/MS och som utnyttjar svagheten att nätet inte kan autentisera meddelanden som tas emot över radiogränssnittet. Användaren luras in på den falska BS/MS. När användaren eller inkräktaren börjar med ett samtal, låter nätverket bli att kryptera genom att inkräktaren lurar krypteringskommandot. Efter det kan inkräktaren upprätta sin egen förbindelse med det verkliga nätverket med sitt eget abonnemang. Inkräktaren kan därefter tjuvlyssna på all dataöverföring som används.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

Ett obligatoriskt krypteringskommando med meddelanden som autentiseras och som hindrar upprepning som tillåter mobilen att verifiera krypteringen så det inte blockeras av inkräktaren.

7.5.2 *Eavesdropping on user data by suppression of encryption between the target user and the true network*

En attack som kräver modifiering av BS/MS och som utnyttjar svagheten av att meddelanden inte kan autentiseras av nätverket när de tas emot över radiogränssnittet. Användaren luras till att ansluta till den falska BS/MS. När användaren har startat en förbindelse, modifierar den falska BS/MS krypteringsmöjligheter av MS för att det ska verka som om det finns en inkompatibilitet mellan nätverket och mobilen. Nätverket kan sedan besluta om att upprätta en okrypterad förbindelse. Efter beslutet att inte kryptera, kan inkräktaren tjuvlyssna på användarens data

Hindrar 3G:s säkerhetsarkitektur attacken: JA

En mobilstation med meddelandeautentisering och spärr mot återanvändning tillåter nätverket att verifiera att krypteringen inte har förhindrats av inkräktaren.

7.5.3 ***Eavesdropping on user data by forcing the use of a compromised cipher key***
En attack som kräver modifiering av BS/MS och att inkräktaren till sin förfogande har en falsk autentiseringsvektor och därför utnyttjas svagheten att användaren inte har kontroll över krypteringsnyckeln. Användaren lockas till den falska BS/MS. När användaren eller inkräktaren påbörjar en tjänst, tvingar den falska BS/MS användaren att använda den falska krypteringsnyckeln på användarens mobil tills man upprättat förbindelsen med det verkliga nätverket utnyttjande sitt eget abonnemang

Hindrar 3G:s säkerhetsarkitektur attacken: JA

Användandet av sekvensnummer i anropet tillåter USIM att verifiera färskheten hos krypteringsnyckeln för att skydda mot återanvändning av kompromitterad autentiseringsvektor. Arkitekturen ger inte skydd mot påtvingad användning av en falsk autentiseringsvektor som ännu inte har använts för att autentisera USIM. Därför är nätverket fortfarande sårbart för attacker som utnyttjar möjligheten att använda falsk autentiseringsvektor vilken har detekterats mellan skapandet i autentiseringscentret och användningen i nätverket.
Användaren måste ha förtroende för SN för att på säkert sätt kunna behandla autentiseringsvektorn. Exempelvis kan en inkräktare med falsk BS tränga sig in hemligt med en SN för att få tag på oanvända autentiseringsvektorer, annars kan SN utsätta sig själv för onödig risk genom att lagra ett stort antal autentiseringsvektorer innan de behöver användas.

7.6 Impersonation of the user

7.6.1 *Impersonation of the user through the use of by the network of a compromised authentication vector*

En attack som kräver modifiering av MS och tillgång till en autentiseringsvektor vilken är tänkt att användas för att autentisera användaren. Inkräktaren använder dessa data för att låtsas vara användaren inför nätverket.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

Användandet av sekvensnummer i anropet betyder att autentiseringsvektorerna inte kan återanvändas för att autentisera USIM. Det bidrar till att minska användningsmöjligheterna för att utnyttja en falsk autentiseringsvektor för att efterlikna användaren. Dessa nätverk är dock fortfarande sårbara för attacker som använder falska autentiseringsvektorer vilka har detekterats mellan skapandet i autentiseringscentret och användandet i nätverket.

Användaren måste ha förtroende för SN för att på ett säkert sätt kunna behandla autentiseringsvektorn. Exempelvis kan en inkräktare med falsk BS tränga sig in hemligt med en SN för att få tag på oanvända autentiseringsvektorer, eller kan SN utsätta sig själv för onödig risk för att lagra ett stort antal autentiseringsvektorer innan de behöver användas.

7.6.2 *Impersonation of the user through the use by the network of an eavesdropped authentication response*

En attack som kräver modifiering av MS och som utnyttjar svagheten att en autentiseringsvektor kan användas flera gånger. Inkräktaren tjuvlyssnar på autentiseringssvaret som användaren har skickat och använder svaret när samma anrop skickas igen sedan. Därefter måste krypteringen undvikas med någon av metoderna som är beskrivna ovan. Inkräktare utnyttjar de avlyssnande svarsdata för att låtsas vara användaren gentemot nätverket.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

Användningen sekvensnummer i anropet betyder att autentiseringsvektorerna inte kan återanvändas för att autentisera USIM.

7.6.3 *Hijacking outgoing calls in networks with encryption disabled*

Denna attack kräver modifiering av BS/MS. Medan användaren ligger på den falska basstationen, avvaktar inkräktaren användarens inkommande samtal. Sedan förbereder användaren ett samtal, vilket inkräktaren tillåter ske mellan nätverket och användaren. Detta får det att från nätverket sett ut som om användaren sätter igång ett mobilsamtal. Nätverket kan sedan upprätta en okrypterad förbindelse. Efter autentisering bryter inkräktaren förbindelsen med användaren, och därefter används förbindelsen med nätverket för att genomföra olagliga samtal på användarens konto.

Hindrar 3G:s säkerhetsarkitektur attacken: DELVIS.

Integritetsskydd för kritiska meddelanden skyddar mot attacken. Närmare bestämt gör dataautentisering och upprepningshinder av begäran om att få starta en förbindelse, att nätverket kan verifiera att denna begäran är legitimerad. Periodiska integritetsskyddade meddelanden under förbindelsen hjälper till att skydda mot kapningar av okrypterade förbindelser, efter den första förbindelseetableringen. Men kapning av kanalen mellan de periodiska integritetsskyddade meddelandena är fortfarande möjlig, även om det kan vara av begränsat intresse för inkräktare. I allmänhet är förbindelser med krypteringen avstängd alltid sårbara (till viss del) för kanalkapning.

7.6.4 Hijacking outgoing calls in networks with encryption enabled

Denna attack kräver modifiering av BS/MS. Förutom det som ingick i föregående attack, måste inkräktaren försöka hindra kryptering genom att modifiera meddelandet vilket gör att MS informerar nätverket om sin krypteringsförmåga.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

7.6.5 Hijacking incoming calls in networks with encryption disabled

Denna attack kräver modifiering av BS/MS. Medan användaren är ansluten till den falska basstationen, gör en medhjälpare till inkräktaren ett samtal till användaren. Inkräktaren beter sig som vidarebefordrare mellan nätverket och användaren tills autentisering och initiering av ett samtal verkställts mellan användaren och nätverket. Nätverket möjliggör inte kryptering. Efter autentisering och samtal start så släpper inkräktaren användaren, och därefter används förbindelsen till att svara på samtalet som kommer från hans medhjälpare. Användaren är tvungen att betala för dessa olagliga samtal.

Hindrar 3G:s säkerhetsarkitektur attacken: DELVIS

7.6.6 Hijacking incoming calls in networks with encryption enabled

Denna attack kräver modifiering av BS/MS. Förutom det som ingick i föregående attack, måste inkräktaren försöka hindra kryptering.

Hindrar 3G:s säkerhetsarkitektur attacken: JA

8 Framtida mobiltelefoni 4G

4G, fjärde generationens mobiltelefoni (eller vad det nu kommer att kallas i framtiden), är ett fullständigt IP baserat mobilintegrerad system som har åstadkommits efter att man har kombinerad trådade och trådlösa nätverk liksom dator, elektronik, kommunikationsteknologi och andra teknologier. Systemet är kapabelt till en överföringshastighets som ligger mellan 100 Mbit/s och 1 Gbit/s, (respektive utomhus och inomhus miljö) med Quality of service (QoS) hela vägen ut och hög säkerhet. Tekniken erbjuder vilken tjänst som helst, när som helst, var som helst, och en debitering som man har råd med.

Wireless World Research Forum (WWRF) definierar 4G som ett nätverk som fungerar med Internet-teknologi, som kombineras med andra applikationer och teknologi liksom Wi-Fi och WiMAX. Den fungerar med hastigheter från 100Mbit/s (inom mobila nätverk) till 1 Gbit/s (inom lokal Wi-Fi nätverk). 4G är inte bara en definierad teknologi eller standard, utan en samling av teknologier och protokoll som möjliggör en hög överföringshastighet och en låg kostnad med möjlighet till trådlösa nätverk.

För att upprätthålla kvalitet hos tjänsten och hastighetskrav har nya applikationer infört som trådlös bredband access, Multimedia Messaging Service(MMS), video chat, mobila TV, HD TV, DVB och minimala tjänster som röst och data när som helst och var som helst. 4G arbetsgruppen har definierat följande som mål för 4G:s trådlösa kommunikationsstandard. Standarderna är:

- Ett effektivt bandbreddsutnyttjande system(inom bitar/s/Hz och bitar/s/Hz/plats).
- Hög nätverkskapacitet.
- En nominell datahastighet på 100Mbit/s vid hög hastighet och 1 Gbit/s vid stationärt tillstånd som definieras av ITU-R.
- En datahastighet av åtminstone 100 Mbit/s mellan vilka två punkter i världen.
- Mjuk handskakning över ett heterogen nätverk.
- Gränslös, förbunden och global roaming över multipelt nätverk.
- Hög kvalitet hos tjänster för nästa generations multimedia support (realtids-audio, höghastighets data, HDTV video innehåll, mobila TV, etc).
- Möjligheten att arbeta tillsammans med existerande trådlösa standarder.
- Ett all IP-baserad paketförmedlande nätverk.

9 Slutsats

3G står för ”tredje generationens mobiltelefoni” och är efterträdaren till dagens mobilsystem GSM. Den stora skillnaden handlar om hur mycket information nätverket klarar av att överföra. GSM är gjort för röstkommunikation, vilket kräver ganska lite information.

3G är däremot även skapat för videotelefoni, och då ställs betydligt högre krav. Det betyder även att 3G är perfekt för att surfa på Internet, på samma sätt som nätet klarar av ljud och video hanterar det förstås även text och bild. Abonnenterna skall kunna ringa och överföra data med förtrogenhet att ingen skall kunna tjuvlyssna eller få tag på data. Därför är säkerheten är en viktig del inom UMTS. Stora nyckellängder, starka krypteringsalgoritmer och utbyggnad av integritetsskydd bidrar till att göra säkerhetsnivån hos UMTS bättre än GSM.

Som har framgått under rubriken attacker så har flera återgärder tagits i UMTS där flera av attackerna var stora risker i GSM. Det har kommit nya attacker i UMTS som inte påträffades i GSM vilket beror på att UMTS är en IP-baserad telefoni som kan anslutas till Internet där riskerna är stora för attacker.

Säkerhetsaspekterna av UMTS står för data konfidentialitet och integritet, identitetsautentisering och användarkonfidentialitet. Men det finns fortfarande undantag som inkräktare utnyttjar. Framtidens 4G mobiltelefoni skall förhoppningsvis kunna täcka dessa undantag som har mer komplicerade algoritmer och säkerhetsaspekter.

10 Referens

[1]
Valtteri Niemi och Kaisa Nyberg: UMTS SECURITY, John Wiley & sons, Ltd, 2003.

[2]
Tredje generationens mobiltelefonisystem UMTS. En studie av radioaccesstekninken WCDMA.
Av: Tomas Axelsson/Luleå universitet

[3]
http://www.3g4g.co.uk/Tutorial/ZG/zg_security.html
Datum: 2007-03-20
Tid: 12:00

[4]
http://www.umtsworld.com/technology/security.htm
Datum: 2007-03-22
Tid: 14:36

[5]
http://books.google.com/books?hl=sv&lr=&id=-3kBJEE28kcC&oi=fnd&pg=PR11&dq=information+about+security+in+UMTS&ots=HvxJPUqgY5&sig=NtvT0CdUVFq3cwS8DuBiaAZZTuU#PPP1,M1
Datum: 2007-03-28
Tid: 09:45

[6]
http://www.cse.wustl.edu/~jain/cse574-06/ftp/cellular_security/index.html
Datum: 2007-03-30
Tid: 03:23

[7]
http://www.cs.tu-berlin.de/~jutta/gsm/js-intro.html
Datum: 2007-03-30
Tid: 01:11

[8]
http://www.gsm-security.net/gsm-security-papers.shtml
Datum: 2007-04-01
Tid: 12.55

[9]
http://sv.wikipedia.org/wiki/UMTS
Datum: 2007-04-04
Tid: 14:22

[10]
http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System
Datum: 2007-04-08
Tid: 20:33

[11]
http://www.umtsworld.com/technology/overview.htm
Datum: 2007-04-13

[12]
http://www.3gpp.org/
Datum: 2007-04-18
Tid: 11:48

[13]
Security for the Third Generation (3G) Mobile System
Av: Colin Blanchard/ London

[14]
A Contemporary Foreword on GSM Security
Av: Paulo S. Pagliusi/ London

[15]:
Introduction to 3G Mobile Communications
Av: Juha Korhonen/London

[16]
Security in mobile phone systems
Av: Alexandre Lung-Yut-Fong and Boris Granovskiy

11 Appendix A

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
A3	Derivation function for RES user in GSM authentication
A5	Confidentiality algorithm used in GSM
A8	Derivation function for Kc used in GSM
AH	Authentication Header
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AMPS	Advanced Mobile Phone System
AUTN	Authentication Token
AV	Authentication Vector
CDMA	code division multiple access
CK	Cipher Key
ESP	Encapsulating Security Payload
f1	Message authentication function used to compute MAC
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK
f8	3G ciphering function
f9	3G integrity function
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HE	Home Environment
HLR	Home Location Register
HSDPA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
IKE	Internet Key Exchange
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
Iu	Interface between MSC/SGSN and RNC
Iub	Interface between RNC and BS
Iur	Interface between RNS:s
KAC	Key Administration Centre
IMT-2000	International Mobile Telecommunications-2000
MAC	Message Authentication Code
ME	Mobile Equipment

MS	Mobile Station
PRP	Pseudo Random Permutation
RAND	Random challenge
RES	Response
RKA	Related Key Attack
RNC	Radio Network Controller
SA	Security Association
SEG	Security Gateway
SQN	Sequence number
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SN	Serving Network
TD-CDMA	Time Division - Code Division Multiple Access
TD-SCDMA	Time Division - Synchronous Code Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UICC	UMTS IC Card
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
Uu	Radio interface
VLR	Visitor Location Register
W-CDMA	Wideband Code Division Multiple Access
XMAC	Expected Message Authentication Code
XRES	Expected Response
XOR	Exclusive OR