Università degli Studi di Perugia

Facoltà di Scienze Matematiche Fisiche e Naturali

Corso di Laurea Specialistica in Informatica

Seminario del corso di Sicurezza

Sicurezza nei sistemi mobile

Studente:
Ambus Giuliano

Docente:
Stefano Bistarelli

Indice generale

Introduzione

Lo scopo di questo seminario è quello di illustrare le caratteristiche dei sistemi Mobile e in particolare darne una descrizione in termini di sicurezza ovvero delle tecniche adottate per rendere la comunicazione sicura. Verranno quindi prese in considerazione le reti GSM , UMTS e WLAN il protocollo Mobile IPv6 e infine un breve accenno alla tecnologia bluetooth.

Lo sviluppo di una tecnologia *mobile* in grado di offrire un buon sistema di comunicazione e innovativi servizi è avvenuta durante la cosi detta "seconda generazione" della telefonia cellulare e tale sistema è arrivata pian piano fino alla terza e ora quarta generazione offrendo un maggior numero di servizi e applicazioni sfruttando varie tecnologie.

Ma la disponibilità di questi servizi *mobile* ha posto vari problemi di sicurezza. Ad esempio un messaggio trasmesso tramite un canale radio (come un SMS) può essere intercettato da terze parti e modificato o la possibilità di accedere a un sistema sfruttando un errore nel protocollo della rete.

L'obiettivo di questo seminario è quindi quello di , dopo aver dato una breve panoramica su cosa siano il sistema GSM e UMTS , definire quali siano gli obiettivi di sicurezza usati in tali reti e come raggiungerli; illustrare gli algoritmi di crittografia usati nel sistema mobile e nel protocollo Mobile IPv6 e infine dare un quadro generale sulla sicurezza nelle reti *wireless.*

1. Tecnologia mobile e sistema GSM

La comunicazione mobile è tecnicamente un servizio che consente a due utenti di stare in comunicazione tra loro pur trovandosi uno o entrambi in movimento.

Tale esigenza fu da sempre richiesta , in primo luogo in ambiti militari e pubblici , e lo sviluppo vero e proprio di una simile tecnologia si ebbe con l'introduzione delle tecniche di modulazione di frequenza (FM – Frequency Modulation) nel 1935 ad opera di E.H. Armstrong. Tali sistemi usavano un singolo canale FM per ogni comunicazione (di ampiezza 120 Khz) e tipicamente la comunicazione poteva coprire una zona ristretta. Ogni utente operava quindi su una propria banda e il numero di canali disponibili erano limitati.

Erano quindi notevoli i problemi di sicurezza , in quanto vi era la possibilità di intercettare le chiamate e non esisteva una procedura di autenticazione.

Una miglioria a questo primo sistema avvenne con l'introduzione del *sistema cellulare*. In breve secondo questo sistema il territorio viene diviso in celle come mostrato in figura dove ogni cella contiene una stazione radio base BTS che gestisce un certo numero di frequenze e di utenti all'interno di una singola cella.

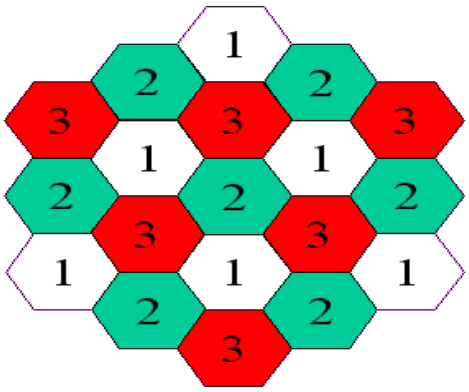


Fig.1-Suddivisione del territorio in celle

Sostanzialmente tale sistema funziona cosi: l'utente di una cella che vuole comunicare con un' altro utente (magari in un'altra cella) si collega e invia i dati alla BTS (Base station Tranceiver) della sua cella che poi invierà la comunicazione alla BTS della cella dell'utente destinatario e quindi al destinatario. Con i sistemi cellulari si ricorre alla tecnica del riutilizzo delle frequenze, cioè, una frequenza si utilizza più volte in luoghi diversi, sufficientemente lontani tra loro, in modo da evitare interferenze e da poter così avere più canali a disposizione .

Ciò che accade quando l'utente si sposta da una cella ad un'altra, è che necessariamente con il suo terminale mobile deve sintonizzarsi su una nuova frequenza, tipicamente quella ricevuta meglio tra tutte le frequenze della nuova cella. Questa operazione prende il nome di *handover*.

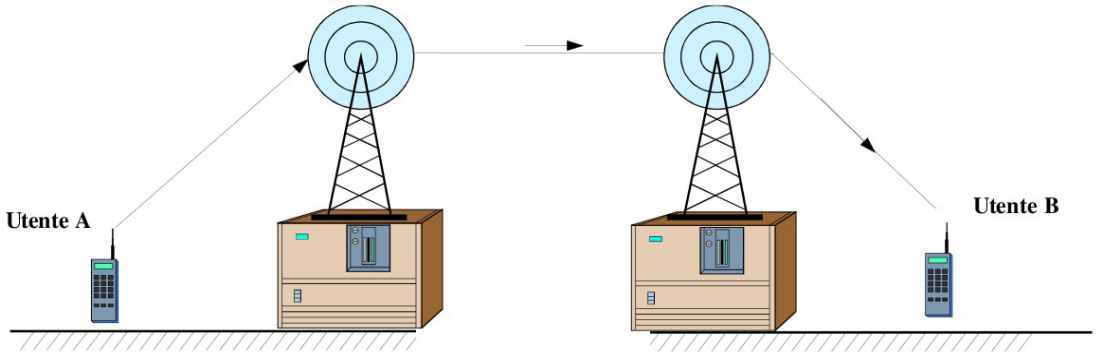


Fig.2-Esempio di comunicazione tra due utenti

I primi sistemi cellulari erano analogici e rappresentano quindi la prima generazione mobile e risalgono agli inizi degli anni 80.Bisogna, però, attendere ancora qualche anno (1985) perché anche nel Regno Unito vengano introdotti i sistemi cellulari analogici conosciuti come TACS (Total Access Communications System).

Tale sistema di tipo analogico che rappresenta la prima generazione di telefonia mobile e si basava su determinate caratteristiche e ad ogni utente che intendeva comunicare veniva assegnata una frequenza portante che rimaneva invariata per tutta la durata della conversazione. Questo metodo prende il nome di multiplazione di frequenza (FDMA Frequency Division Multiple Access) ed è uno dei tre metodi utilizzati nelle trasmissioni ad accesso multiplo. La comunicazione era di tipo full duplex , ma non era previsto nessun sistema di autenticazione (solo un riconoscimento su un codice dell'apparecchio detto IMEI), e nessuna possibilità di inviare dati.

Come possiamo notare tale sistema era molto limitativo e la tecnologia presentava notevoli problemi di sicurezza come il fatto che non vi sia una crittografia sulla comunicazione o il fatto che l'accesso alla rete è basato sulla verifica di un semplice codice (IMEI).

L'evoluzione di questo sistema ha portato alla seconda generazione di telefonia mobile nota come sistema GSM.

1.1 Il sistema GSM

Lo sviluppo della telefonia mobile di tipo analogico fecce si però che ogni nazione sviluppasse una propria rete di comunicazione e per chi era dotato di telefonini TACS la comunicazione restava racchiusa all'interno dei confini nazionali.

Si decise così tra il 1982 e il 1985 di dare vita a un sistema di comunicazione digitale e pan-europeo in modo da garantire non solo una comunicazione dei dispositivi a livello europeo , ma di creare anche una sorta di concorrenza tra i vari fruitori del servizio in modo da abbatterne i costi di servizio.

Nel 1982 quindi venne creato gruppo di studio *Group Special Mobile* con lo scopo di dare vita a un sistema di comunicazione mobile a livello europeo e più sicuro del tradizionale sistema analogico. Tale sistema doveva garantire dei servizi migliori rispetto al precedente standard e gli obiettivi che si prefissarono furono:

- ✔ Assicurare una buona comunicazione audio
- ✔ Bassi costi per terminali e gestione del servizio
- ✔ Possibilità di *roaming* internazionale
- ✔ Introduzione di nuovi servizi
- ✔ Maggiore sicurezza nelle comunicazioni
- ✔ Compatibilità col servizio ISDN

Dopo aver definito tali obiettivi e stabilito che il sistema doveva essere di tipo digitale nacque così il sistema GSM assegnando per tale servizio due bande , una tra gli 890 e i 915 Mhz e un altra tra i 935 e i 960 Mhz (una per l'up-link e una per il down-link).

L'uso di una tecnologia digitale permise notevoli vantaggi , infatti il segnale vocale *viene* codificato in bit e inoltrato attraverso un canale radio-telefonico, offrendo quindi la possibilità di criptare i messaggi trasmessi o di cifrare l'identità dell'utente o ancora di inviare dati oltre che segnali vocali (servizio sms ad esempio).

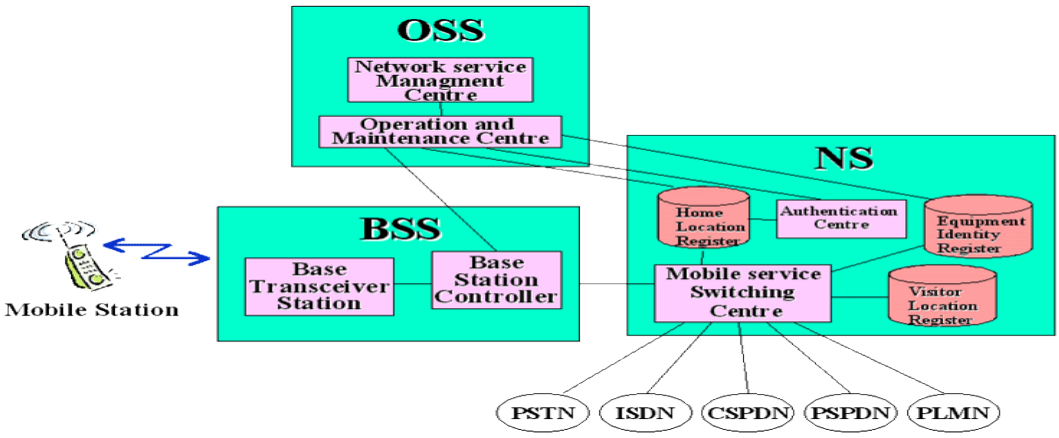
Definite tutte le specifiche nel 1987 la responsabilità per il sistema GSM venne affidata all' *European Telecommunication Standards Institute* (ETSI) , ovvero l'ente che si occupò di definire tramite normative tutte le specifiche standard del sistema GSM e che rinomino l'acronimo GSM come *Global System for*

Mobile Comunication. Questa fu la così detta *fase 1* del sistema GSM e che si concluse nel 1991.

Gli obiettivi generali di sicurezza posti dal sistema GSM , e che vedremo come sono stati realizzati , sono evitare un uso non autorizzato del servizio,la protezione dei dati trasmessi, e l'autenticazione degli utenti , evitare l'intercettazione delle comunicazioni.

1.2 Componenti del sistema GSM

Vediamo quindi le componenti fondamentali del sistema GSM. L'architettura della rete GSM è cosi posta:



Vediamo le componenti principali :

- **MS (Mobile Station)** : Rappresenta l'apparecchio telefonico o meglio lo strumento per comunicare.

  Tecnicamente è composto da *Mobile Equipment* (ME) cioè il telefonino vero e proprio e la SIM (*Subscriber Identity Module*) card. Questa ultima è fondamentale e contiene tutte le informazioni per l'utente (numeri di telefono, messaggi, ecc...) e per l'autenticazione contiene infatti il codice IMSI (*International Mobile Subscriber Identity*) per identificare l'utente, il codice TMSI (*Temporary Mobile Subscriber Identity*) e la Ki la chiave segreta di autenticazione. La scheda contiene poi l'algoritmo di cifratura usato nel sistema (A8) e l'algoritmo di autenticazione (A3), e infine dei codici (PIN e PUK) che consentono al solo possessore (l'utente proprietario della SIM) di accedere alla scheda. Il ME invece è identificato in modo univoco tramite il codice IMEI (*International Mobile Equipment Identity*).

- **BSS (Base Station Subsistem):** Tale struttura è composta da BTS (Base Tranceiver Station) ovvero una stazione radio base con cui la MS comunica direttamente , e dal BSC (Base Station Controller) che agisce come nodo comune tra le varie BTS nella rete.

- **NS (Network Subsystem):** E' costituito da una serie di componenti ovvero e rappresenta la Network System:

  - MSC (*Mobile Switching Center*) che è collegato direttamente alle BSC e permette la comunicazione tra gli MS e le normali reti pubbliche (PSTDN,ISDN ecc...)
  - HLR (*Home Location Register*)è in sostanza un database che contiene informazioni circa l'abbonato e i suoi dati di abbonamento.
  - VLR(*Visitor Locator Register*) : è un database interrogato dal' MSC che contiene le informazioni delle MS che si trovano sotto quell'area della rete da esso servito.
  - AUC (*Autentication Center*): è l'unità funzionale del sistema GSM, incaricata di generare i parametri necessari per l'autenticazione degli utenti, che poi fornisce all' HLR. Si occupa di verificare se il servizio è stato richiesto da un abbonato leggittimo, fornendo sia i codici per l'autenticazione che per la cifratura. L'AuC contiene: il codice IMSI (*Interntional Mobile*

Subscriber Identity), la chiave di autenticazione (*Ki*), il codice TMSI (*Temporary Mobile Subscriber Identity)* corrente ed il codice LAI (*Location Area Identity*) corrente, usati per autenticare i canali radio, oltre ad un generatore di numeri casuali, agli algoritmi A3 e A8.

- EIR(*Equipment Identity Register*): è il database dove sono registrati tutti gli *International Mobile Equipment Identity* (IMEI), ciascuno dei quali identifica univocamente un ME.

Come detto sulla SIM sono posti i codici IMSI. Oltre a questi troviamo i codici TMSI cioè delle identità temporanee. All'inizio l'abbonato si autentica usando il proprio IMSI e dopo essersi autenticato gli viene assegnato un codice TMSI trasmesso in maniera crittografata e da quel momento in poi l'utente per identificarsi userà solo il codice TMSI. Tale codice varrà fino a che l'utente si troverà in una certa LA (Location Area), cioè quella zona dove l'utente si può muovere e può comunicare senza dover comunicare ogni volta la propria posizione al VLR. Quando poi un utente si sposta su un area dove il suo TMSI non è riconosciuto gli viene assegnato un nuovo TMSI.

2 Sicurezza nel sistema GSM

2.1 Algoritmi crittografici

Il GSM usa un sistema di crittografia simmetrico per l'autenticazione e per la cifratura dei segnali, viene quindi usata un 'unica chiave per la cifratura e decifratura dei messaggi. L'idea di usare un sistema a chiavi pubbliche venne anche presa in considerazione ma nel 1980 tale sistema non era ancora abbastanza flessibile con la tecnologia richiesta dal sistema GSM.

I tre principali algoritmi di crittografia del sistema GSM sono:

- l'algoritmo per l'autenticazione A3
- l'algoritmo per la cifratura dei messaggi A5
- l'algoritmo per la generazione della chiave A8

Vediamo i vari aspetti di sicurezza da tenere in conto nel sistema.

2.2 Autenticazione e chiavi di sessione

La procedura di autenticazione viene avviata ogni qualvolta la Mobile Station (MS) si collega alla rete, e più precisamente nei seguenti casi:

- ogniqualvolta la MS riceve o effettua una chiamata,
- ogniqualvolta venga effettuato l'aggiornamento della posizione della Mobile Station (Location Updating),
- ogniqualvolta venga effettuata l'attivazione, disattivazione o interrogazione dei servizi supplementari.

Le unità funzionali in gioco nel processo di autenticazione sono: la SIM nel terminale e l'AuC (*Authentication Center*) nella home networkdel GSM . L'autenticazione avviene adottando un meccanismo di tipo challenge-response. Nel momento in cui l'AuC riceve una richiesta di autenticazione, riconosce la probabile identità dell'utente, genera e trasmette al Mobile Equipment (ME) un numero casuale di 128 bit (**RAND**) come sfida (*challenge*). La SIM calcola la risposta (*response*) **SRES** di 32 bit alla sfida dando in input all'algoritmo di autenticazione **A3** (*key-dependent one-way hash function*) il numero casuale (RAND) e la chiave di autenticazione dell'utente Ki, che ha una lunghezza di 128 bit ed è memorizzata nella stessa SIM. La risposta "firmata" SRES viene trasmessa alla visited network dove viene confrontata con il valore che la home network ha calcolato applicando lo stesso algoritmo A3 al numero casuale RAND e alla chiave Ki corrispondente alla identità dichiarata dall'utente (di cui conserva copia).

L'utente è autenticato e può accedere alla rete se e solo se i due valori, quello ricevuto SRES e quello

calcolato coincidono (la SIM è in possesso dell'esatta chiave di identificazione), altrimenti la connessione viene rifiutata e un messaggio di *authentication failure* viene notificato alla Mobile Station. L'immagine sottostante riepiloga ciò che viene eseguito in fase di autenticazione. Notiamo che all'inizio la ME si identifica usando il prorpio IMSI (o TMSI se non è la prima autenticazione).

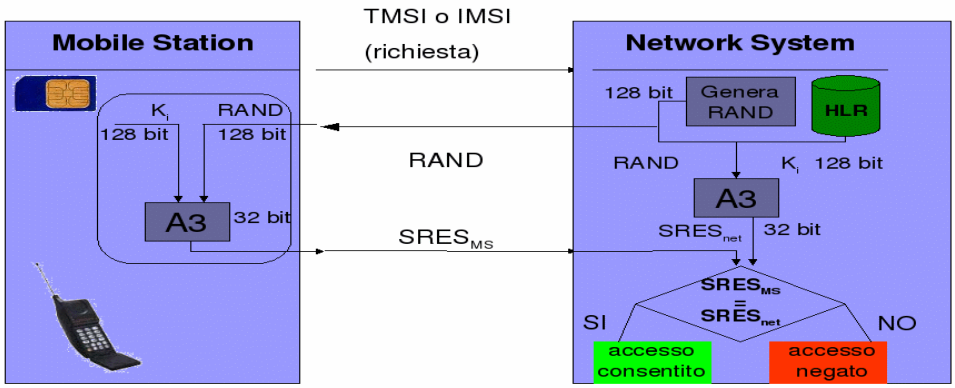


Fig. 3 - Autenticazione

L'algoritmo usato per la generazione delle chiavi di sessione è l'algoritmo A8, il quale genera la chiave Kc tramite la RAND inviata dalla MSC e tramite la propria chiave Ki. Ricapitolando quindi l'utente tramite l'algoritmo A3 genera lo SRES per autenticarsi e tramite l'algoritmo A8 genera la chiave Kc , ovvero la chiave di sessione. Tale algoritmo prende i 128 bit della chiave e del RAND e genera un output a 64 bit.

Oltre a tale algoritmo è stato implementato un altro algoritmo detto COMP128 che invece di eseguire i due algortimi A3 e A8 separatemente, in un certo senso fonde i due e produce un output di 128 bit dove i primi 32 formano la risposta SRES e gli ultimi 54 la chiave Kc.

2.3 Cifratura

Il sistema GSM normalmente cifra i messaggi trasmessi via radio tra la Mobile Station e la Base Tranceiver Station.

Tale viene fatto usando l'algoritmo A5 di seguito definito.

Tale è uno *stream cipher* ovvero un tipo di cifratore che opera bit a bit , nel senso che per ogni bit del testo in chiaro produce il bit codificato in uscita. Sostanzialmente funziona come uno XOR tra i bit in ingresso e una sequenza di bit chiave usati per cifrare (*key stream*) a differenza dei cifrari a blocchi che invece dividono il testo in chiaro in più blocchi e poi cifrano i blocchi usando la stessa chiave.

A5 opera utilizzando come chiave di cifratura la chiave Kc a 64 bit, ottenuta dall'algoritmo A8, e i 22 bit della trama TDMA[1] e ottiene un frame da 114 bit usato per cifrare i primi 114 bit significativi del messaggio da trasmettere.

Per cifrare un messaggio avviene come mostrato in figura ovvero da prima tramite l'algoritmo A8 genera la chiave Kc e che insieme ai 22 bit del frame TDMA genera i 114 bit da usare come chiave per eseguire lo stream cipher ovvero per cifrare i messaggi da trasmettere. L'operazione è eseguita sia nella SIM che nella MSC.

1 Il sistema GSM usa una tecnica detta TDMA time Division Multiple Access per consentire a più utenti di accedere al canale. Tale è una tecnica di multiplazione in cui la condivisone del canale è basata sulla ripartizione del tempo di accesso.

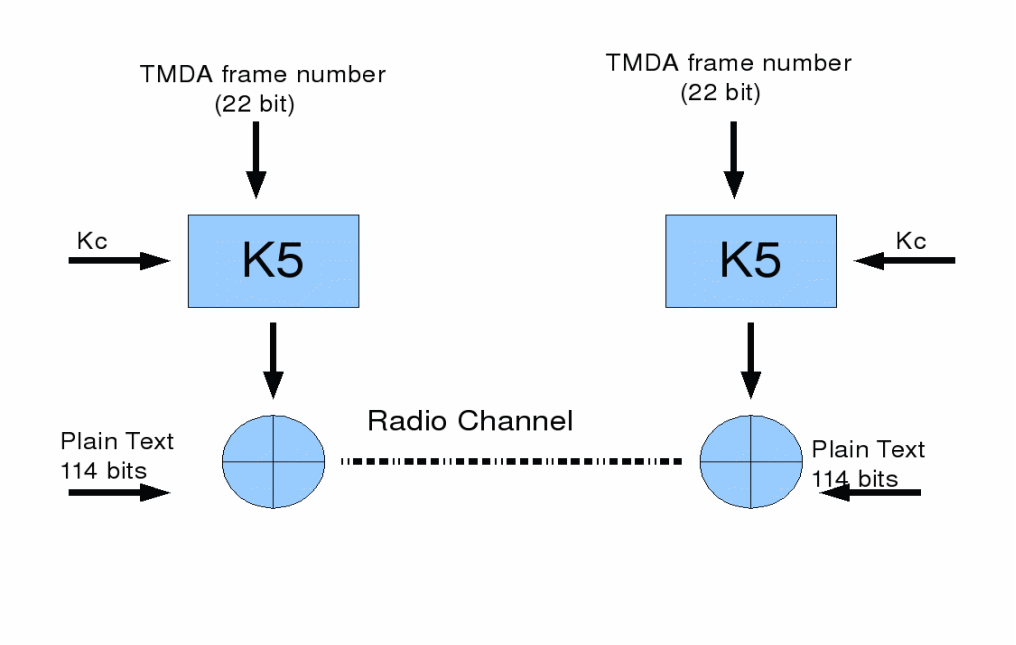


Fig.4 – Cifratura del messaggio

Possiamo notare come neppure la chiave Kc, venga trasmessa sul canale radio o rilasciata dalla SIM. Perciò anche nel caso in cui si riuscisse a superare la procedura di autenticazione, ad esempio manipolando il confronto tra challenge e response, Mobile Station e Base Station utilizzerebbero chiavi di cifratura diverse risultando incomprensibili l'una all'altra.

La chiave Kc è diversa ad ogni collegamento (viene generata una nuova Kc ogni volta che si esegue la procedura di autenticazione), dipendendo da RAND. Un ulteriore livello di sicurezza può essere raggiunto consentendo di modificare la chiave Kc ad intervalli regolari di tempo, secondo le esigenze della rete.

Notiamo poi come venga usato uno stream cipher invece di un block cipher , che è simile solo che opera su blocchi di bit, Un block cipher è poi più pericoloso in caso di errori. Infatti se usiamo uno stream cipher l'errore di un bit crea un errore su un bit del plain text prodotto mentre invece un errore in un bit in sistema di tipo block cipher crea un errore su un intero blocco del plain text.

2.4 Rischi del sistema GSM

Anche se dotato di tali sistemi di crittografia il sistema GSM può subire vari tipi di attacchi e un gruppo di ricercatori dell'Università della California ritiene che la semplicità nel rompere l'A5 sia dovuta al fatto che il governo lo abbia deliberatamente indebolito per fini di sorveglianza delle comunicazioni.

Rompendo il metodo di crittografia GSM, si potrebbe clonare un telefono protetto da tale codifica, cioè rilevare un numero di telefono ed utilizzarlo in una comunicazione fraudolenta da un altro telefono.

Sebbene l'A5 utilizzi una chiave a 64 bit, ricercatori hanno scoperto che gli ultimi 10 bit sono settati a 0 Questo significa che con computer estremamente potenti, a disposizione delle varie agenzie governative, potrebbe essere possibile, abbastanza velocemente, decodificare una conversazione.

Per anni, è girata voce che le industrie di computer siano state persuase o forzate dalle agenzie spia del governo ad indebolire matematicamente i sistemi di sicurezza delle comunicazioni o installare trappole segrete. Alcuni sospetti riguardavano anche l' NSA (National Security Agency), e la CIA (Central Intelligence Agency). L'NSA è una delle agenzie maggiormente sospettate, dato che la maggior parte delle sue missioni è quella di intercettare chiamate telefoniche.

Vediamo comunque i vari tipi di attacco cui può essere soggetto il sistema GSM:

- ATTACCO BRUTE FORCE : Permette , tramite un opportuno algoritmo, di generare tutte le possibili chiavi usate sia per autenticazione che per sessione. É un procedimento lungo (2^54 operazioni) ma non impossibile.
- ACCESSO AI SEGNALI DELLA RETE: l'algoritmo è sicuro abbastanza da prevenire l'intercettazione di chiamate via-etere e la decifratura in real-time. Sfortunatamente, le onde radio tra la MS e la BTS non sono i soli punti vulnerabili nel sistema GSM. Dopo la BTS, i segnali vengono trasmessi in chiaro nelle operazioni di rete .

  Questo apre nuove possibilità. Se l'attaccante può accedere ai segnali degli operatori della rete, egli sarà capace di ascoltare ogni cosa che viene trasmessa, includendo la chiamata telefonica in corso così come, eventualmente, RAND, SRES e K_c.

- RECUPERO DELLA CHIAVE DALLA SIM:La sicurezza dell'intero modello GSM è basata sulla chiave segreta K_i. Se la chiave venisse scoperta l'intero accesso alla rete sarebbe compromesso. Una volta recuperata la chiave K_i, l'attaccante non solo può ascoltare le chiamate dei sottoscrittori, ma anche addebitare le proprie chiamate sul conto dell'abbonato di cui si è recuperata la chiave segreta. SDA e l'ISAAC hanno scoperto un difetto nell'algoritmo COMP128 che rende capaci effettivamente di recuperare la chiave segreta K_i, dalla SIM . L'attacco richiede l'accesso fisico alla SIM ed è di tipo chosen-challange.

  Tale attacco sfrutta le debolezze dell'algoritmo COMP128 in modo da rivelare informazioni circa K_i quando i RAND appropriati gli vengono forniti in input. La SIM può essere attaccata utilizzando un lettore di smart card connesso ad un PC.
- FURTO DELLA CHIAVE VIA ETERE: La chiave può anche essere rubata via etere oltre che direttamente dalla SIM. L'attacco via etere è basato sul fatto che la MS deve rispondere ad ogni challange inviatagli dalla BTS . Un attaccante potrebbe impersonare la BTS legittima inviando alla MS obiettivo delle challenge per risalire alla chiave segreta mediante le risposte a queste challenge.
- FURTO DELLA CHIAVE DALL' Auc :Lo stesso attacco utilizzato per il recupero di K_i da una SIM card può essere utilizzata per recuperare la chiave K_i dall'AuC. Quest'ultimo deve rispondere alle richieste fatte dalla rete GSM e restituire triple valide da utilizzare nell' autenticazione della MS. La procedura di base è identica alla procedura utilizzata nella MS per accedere alla SIM. La differenza è che l'AuC è molto più veloce nel processare le richieste di quanto non lo sia la SIM card.

2.5 Frodi nel sistema GSM

Il pericolo di frodi e di poter quindi usare un servizio a spese di altri nella rete GSM è abbastanza tipico.

La possibilità di frodi avvengono anche grazie al roaming internazionale offerto dal servizio GSM. In poche parole il roaming consiste nella possibilità offerta ad un utente di parlare , inviare dati o accedere a servizi mentre si sposta da una zona geografica a un altra.

Con il roaming internazionale la chiamata dati su un certo abbonato è di solito in ritardo e tale ritardo viene sfruttato dall'attaccante il qual fa deviare la chiamata verso un altro numero magari internazionale e in più può settare il telefono affinché le successive chiamate siano deviate verso altri numeri.

Un altro tipo di frode è detta *premium rate fruade.* In questo sistema l'attaccante propone all'utente un finto servizio con dei numeri di telefono che l'attaccante invita a chiamare. Le chiamate degli utenti adescati sono rigirate verso numero di proprietà dell'attaccante che sfrutta il sistema di tariffazione presente sulla rete per prelevare soldi all'utente durante la chiamata. L'attaccante poi sparisce non appena l'utente si accorge della

frode.

Il principale strumento di difesa contro attacchi simili sta diciamo a livello umano , evitando di rispondere subito a certi numeri che invitano a qualche servizio di cui non ci si fida .

3. Il sistema UMTS

Lo sviluppo di una tecnologia successiva al GSM venne intrapresa già agli inizi del 1990 e tutti i lavori iniziati in quegli anni portarono allo sviluppo della cosi detta tecnologia UMTS (*Universal Mobile Telecomunication System*) che rappresenta le terza generazione della telefonia cellulare mobile.

Il principale organismo per la standardizzazione del sistema UMTS fu il gruppo 3GPP (*3G Partnership Project*) cui parteciparono i rappresentanti di varie nazioni e le prime specifiche furono rilasciate nel 1999.

La rete del sistema UMTS è tutto sommato simile a quella del GSM con la differenza che l'UMTS utilizza un differente sistema di autenticazione più sicuro rispetto a quello del GSM.

Una prima distinzione sta nel fatto che l'UMTS per la trasmissione dei dati non utilizza la tecnologia a commutazione di circuito, ma integra la trasmissione dati a circuito ed a pacchetto il che consente di ottenere servizi diversificati, come connessioni virtuali continue alla rete, modalità alternative di pagamento (ad esempio pagamenti proporzionali al numero di bit trasferiti o alla larghezza della banda impiegata).

L'autenticazione del sistema UMTS, come dicevamo, prevede una mutua autenticazione tra la rete e il sottoscrittore, che per essere identificato usa una USIM (Universal Subscriber Identity Module) posta nel proprio mobile equipment. Tale è un'applicazione che contiene funzioni e dati necessari ad identificare ed autenticare l'utente. In particolare, contiene l'IMSI (International Mobile Subscriber Identity) che serve ad identificare in maniera univoca l'utente, sebbene l'utente può non conoscerne il valore.

L'USIM è implementata insieme ad altre applicazioni in un circuito integrato posto su una carta removibile detta UICC (UMTS Integrated Circuit Card) e inserite nell' UE (User Equipment ovvero l'apparecchio per comunicare).

La mutua autenticazione che si verifica nel sistema UMTS prevede quindi

- un autenticazione tra la rete a la MS
- un autenticazione tra MS (Mobile Station) e rete

Questo tipo di autenticazione non avviene nel sistema GSM (si verifica solo l'autenticazione tra MS e rete) e infatti si corre il rischio di un' attacco basato su una falsa Base Station ovvero la MS non può capire se la richiesta di usare il proprio IMSI per l'autenticazione proviene da una Base Station falsa o autentica rischiando cosi di inviare il proprio IMSI all'attaccante.

Per quanto riguarda l'architettura del sistema UMTS , questa è simile a quella del GSM e le componenti sono pressoché le stesse per cui non le ripetiamo , ma ci concentriamo invece sugli aspetti di sicurezza e le tecniche di autenticazione adottate al fine di rendere sicura la comunicazione.

3.1 Funzioni crittografiche

I membri del 3GPP quando definirono le caratteristiche del sistema UMTS stabilirono una serie di funzioni e di algoritmi crittografici per garantire la sicurezza, in totale furono definite 10 funzioni che qui elenchiamo :

- **f0**: Funzione per la generazione del numero (pseudo) casuale RAND.
- **f1**: Funzione per l'autenticazione della rete. Genera un codice MAC (Message Authentication Code) o XMAC (Expected MAC).
- **f1***: Funzione per l'autenticazione del messaggio di ri-sincronizzazione. Genera un codice MAC-S

(Message Authentication Code - Synchronisation) o XMAC-S (Expected MAC-S).

- **f2**: Funzione per l'autenticazione dell'utente. Genera un codice RES (User Response) o XRES (Expected RES).
- **f3**: Funzione per la generazione della chiave CK (Cipher Key) che viene data in input alla funzione f8
- **f4**: Funzione per la generazione della chiave IK (Integrity Key) passata in input alla funzione f9.
- **f5**: Funzione per la generazione della chiave AK (Anonymity Key) usata nelle normali operazioni.
- **f5***: Funzione per la generazione della chiave AK (Anonymity Key) usata nei messaggi di ri-sincronizzazione.

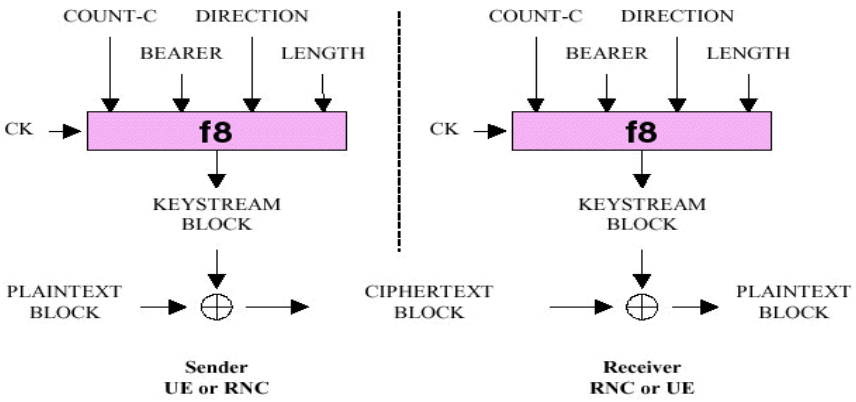
Più due funzioni crittografiche usate per cifrare i messaggi :

- **f8**: Funzione per la riservatezza dei dati. Genera una keystream.
- **f9**: Funzione per l'integrità dei dati. Genera un codice MAC-I (Message Authentication Code - Integrity).

Queste due funzioni hanno compiti specifici , la f8 è la funzione per la riservatezza dei dati (data confidentiality) mentre la f9 è la funzione per l'integrità dei dati (data integrity) e sono state appositamente progettate per l'UMTS, dai partecipanti al 3GPP.

Confidenzialità nell'UMTS

La confidenzialità nel sistema UMTS viene ottenuta facendo uso della funzione crittografica f8 il cui scopo è quello di far si che l'utente e la rete siano gli unici a poter usufruire dei messaggi scambiati. Mediante tale funzione viene generata una keystream che viene poi utilizzata per cifrare i dati. La figura sottostante mostra l'uso dell'algoritmo f8 per cifrare un testo in chiaro mediante l'impiego della keystream.



Viene eseguita un'operazione di xor tra la keystream ed il testo in chiaro; il risultato è un testo cifrato. Dal testo cifrato si può riottenere il testo in chiaro generando la stessa keystream mediante l'utilizzo degli stessi parametri di input ed applicando un'operazione di xor tra la keystream ed il testo cifrato.

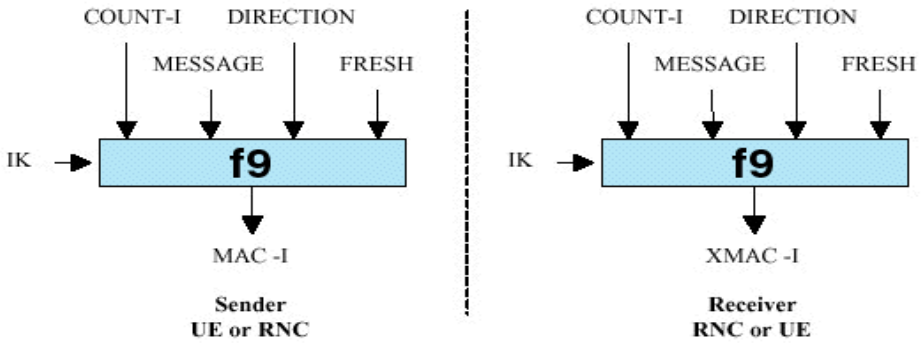
questa funzione accetta in ingresso i parametri

- CK, la chiave di cifratura generata tramite le altre funzioni algoritmiche;
- un contatore COUNT-C, che serve per impedire che la stessa chiave possa essere generata più volte;
- un identificatore *BearerID*, di 5 bit, che indica il *canale* aperto tra i due soggetti;
- un bit di direzione, che indica se si tratta di flusso dati in uplink o in downlink;
- la lunghezza dei blocchi di cifratura, indicata con 16 bit.

La funzione f8 è basata su un algoritmo detto KASUMI. Tale è sostanzialmente un cifrario a blocchi ed è noto anche col nome di A5/3 che opera su blocchi a 64 bit e con chiavi a 128 bit. C'è da dire poi che tale algoritmo dipende da un altro cifrario , il cifrario MYSTY, o meglio KASUMI è il cifrario MYSTY adattato per un implementazione anche hardware.

Integrità nell'UMTS

Per quanto riguarda invece l'integrità questa viene ottenuta facendo uso della funzione crittografica f9. Questa funzione f9 genera un codice di autenticazione dei messaggi denominato MAC-I (Message Authentication Code – Integrity), come mostrato nella figura sottostante



Il codice MAC-I viene aggiunto al messaggio (o dato) di segnalazione MESSAGE quando quest'ultimo viene inviato sui collegamenti radio. Il ricevente calcola il codice XMAC-I utilizzando gli stessi parametri che sono stati utilizzati per calcolare MAC-I da chi ha mandato il messaggio MESSAGE; in particolare il ricevente utilizza come parametro di input anche il messaggio MESSAGE che ha ricevuto. Una volta calcolato XMAC-I, il ricevente lo confronta con il codice MAC-I che ha ricevuto insieme al messaggio; se i due codici coincidono vuol dire che il messaggio MESSAGE non ha subito alterazioni.
La funzione f9 (che come la f8 si basa su KASUMI) accetta in ingresso tali parametri:

- IK, la chiave d'integrità appositamente generata;
- un contatore *COUNT-I*;
- il messaggio da proteggere;
- un bit di direzione;
- un *FRESH*, un numero di *nonce* che viene mandato dalla rete al terminale mobile, prima che inizi la cifratura dei dati, per prevenire *replay attack*.

Tutti gli algoritmi dell'UMTS sono stati pubblicati e testati tramite procedure di crittoanalisi.

3.2 Autenticazione nell'UMTS

Passiamo quindi a vedere come avviene l'autenticazione nel sistema UMTS secondo il protocollo detto AKA (Authenticaton and Key Agreement) che ha come obiettivo quello di

- Far si che utente e rete raggiungano una reciproca autenticazione sulla base di una chiave condivisa.

  memorizzata nella USIM dell'utente e nell'AuC.
- Generare le chiavi per garantire la confidenzialità e l'integrità (da usare negli algoritmi f8 e f9(visti prima).

Quando un apparecchio vuole collegarsi alla rete, manda una richiesta al server MSC/VLR (nel caso di device voce) o al server SGSN/VLR (nel caso di richieste dati). Il server contattato inoltra la richiesta dell'identità del terminale, il quale risponde presentando come credenziale il proprio codice IMSI, che non viene in alcun modo protetto.

Soltanto a questo punto il terminale, con il server VLR ed il server HLR/AuC eseguono il protocollo AKA. Successivamente, se il terminale si sposta di zona, allora ci sarà una *location update* tra i server VLR e HLR. Il numero IMSI, in questa maniera viene trasmesso all'interno della rete locale in cui si trova l'utente: questo comportamento è necessario perché il numero IMSI non è presente nel database locale del server VLR; al contrario, dopo la prima autenticazione, verrà accordata una credenziale temporale TMSI da usare per le successive segnalazioni, così come avviene similmente nel GSM.

All'interno della SIM del device vengono salvati:

- le credenziali IMSI (di lungo periodo), TMSI e P-TMSI (temporanee, per voce o dati);
- una *pre-shared key K*, condivisa tra la SIM e il server AuC.

La *pre-shared key K* è l'unica credenziale usata per autenticare la rete al *mobile device*.

Quando un terminale entra nella zona di pertinenza di un certo VLR, questo manda al server HLR/AuC la richiesta di identificazione del terminale, indicando l'IMSI da autenticare. Il server AuC, in risposta alla richiesta di autenticazione, genera un numero RAND (per il challange) e risponde con un elenco di *Authentication vector AV* ovvero una serie di parametri da usare per l'autenticazione dell'utente. Tali vettori contengono il campo XRES generato usando la funzione **f2** applicata al numero RAND e alla chiave K, la chiave CK a 128 bit ottenuta tramite la funzione **f3** applicata sempre al RAND e alla chiave K, la chiave IK tramite la funzione **f4** e una chiave a 48 bit AK ottenuta applicando la funzione **f5** al numero RAND e alla chiave K.

L'AuC tramite la funzione **f1** e il numero RAND genera il numero MAC e il numero di sequenza SEQ e l'AMF (Authentication Management Filed) e con tutti questi parametri costruisce il numero che servirà al terminale per autenticare la rete e cioè il numero AUTN = <SQN$\oplus$AK,AMF,MAC>.

Quindi crea il vettore <RAND,AUTN,XRES,CK,IK> che invia al VLR e che questi memorizzerà associandolo all'IMSI che ha richiesto l'autenticazione.

A questo punto, il server VLR invia al terminale una richiesta di autenticazione in cui viene inserita la challange RAND e il vettore AUTN.

Quando riceve tale messaggio la USIM (subscriber) per prima cosa calcola AK usando la funzione f5 e passandole come dati il RAND e la chiave K, poi calcola SQN ponendo in xor il valore di AK con il valore presente in AUTN ovvero SQN$\oplus$AK e quindi ottiene SQN = (SQN$\oplus$ AK) $\oplus$AK.

L'USIM a questo punto può determinarsi un XMAC facendo uso dell'SQN generato in precedenza , del RAND passatole e dell'AMF passatole sempre nell'AUTN dal VLR e poi confronta tale XMAC con quello passatogli. Se corrispondono l'USIM autentica la rete altrimenti rifiuta e chiude la connessione.

Se corrispondono per l'USIM è una garanzia del fatto che sia il numero AUTN che il numero RAND sono stati generati dall'AuC a cui la USIM è già stata autenticata e non invece da un impostore.

Infine la USIM genera i parametri RES, CK e IK tramite rispettivamente le funzioni f2,f3,f4 , passando come parametri RAND e la chiave K e li passa alla VLR la quale verifica che il valore di RES sia uguale a quello che ha nel suo vettore di autenticazione (XRES) passatole dall'AuC. Se corrispondono la USIM viene autenticata.

Come si è potuto vedere si è eseguita quindi una mutua autenticazione. Dapprima il subscriber ha autenticato la rete, quindi la rete ha autenticato l'utente.

4 Sicurezza dell'IPv6 mobile

Il problema principale della sicurezza nelle reti GSM e UMTS è essenzialmente controllare l'accesso a un servizio quando l'utente è in movimento e non ha ancora stabilito un collegamento con l'operatore della rete che offre il servizio.

Cercheremo ora di mostrare un altro problema di sicurezza relativo alle reti mobile ovvero, il sistema detto

Mobile IPv6.

Brevemente diciamo che Mobile IP è un standard IETF di comunicazione che è stato progettato per consentire agli utenti di dispositivi mobili (essenzialmente portatili) di passare da una rete all'altra, pur mantenendo un indirizzo IP e essere comunque raggiungibili. In sostanza tale tecnologia deriva direttamente dai protocolli IPv4 e IPv6 solo che mentre nella rete fissa non ci sono problemi, ovvero a un utente si assegna un IP , ma l'utente non si muove, in caso di mobilità invece è necessario quando l'utente si sposta su un altra sotto-rete assegnare un nuovo IP altrimenti l'utente resta irraggiungibile. Il protocollo "IP-Mobile" consente di superare questo vincolo, facendo sì che nodi mobili, con pre-assegnati indirizzi IP, possano continuare a comunicare al variare del proprio "Current Point of attachment" senza modificare il proprio indirizzo.

Sorgono però dei problemi di sicurezza.

Il problema di fondo sta nel capire quando un device cambia la sua posizione nella rete , come possono gli altri nodi stabilire se la posizione dichiarata dal device è quella in cui realmente si trova e dichiarata.

Nelle reti cablate sapiamo che un nodo può mentire circa la sua identità (dichiarando o usando un falso IP), nelle retei mobile un nodo può mentire non solo circa la sua identità ma anche circa la sua posizione riuscendo cosi a generare certi attacchi vediamo perché.

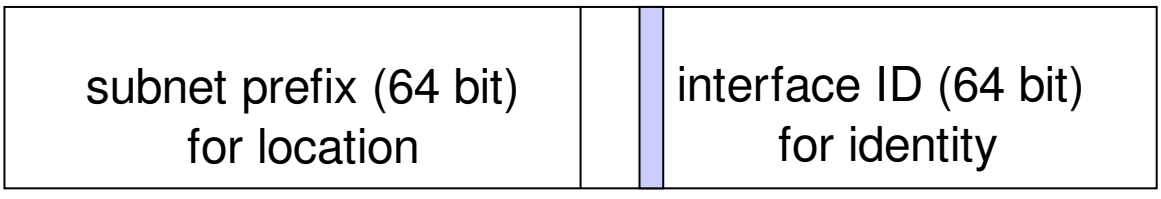
Ad esempio Alice può dichiarare di essere nella locazione in cui si trova Bob in modo da far si che tutti i messaggi diretti a Bob siano invece girati a lei o ancora può dire che Bob si trova in una certa locazione che però in realtà non esiste e far perdere tutti i pacchetti a lui indirizzati.

Un 'altro tipo di attacco , detto *Bombing Attack* , si verifica nel caso in cui Alice dichiara di trovarsi nella stessa locazione di Bob, quindi ordina una grande quantità di traffico che invece fa poi girare verso Bob causando un Denial of Sevice. In tal caso verificare che le informazioni circa la posizione di Alice siano corrette non basta perché le informazioni giungono da lei Alice solo che Alice mente circa la sua posizione.

4.1 Mobile IPv6

La diffusione e la diversificazione dei dispositivi wireless (computer portatili, palmari, telefoni cellulari, e le relative tecnologie (infrarossi, onde radio, …) capaci di offrire servizi di connettività, stanno mutando radicalmente il concetto di punto di "attacco" di un nodo ad Internet. I dispositivi mobili, per loro natura, vorrebbero essere indipendenti dalla rete cui sono connessi senza compromettere le loro usuali configurazioni di rete e le connessioni con host che non adottano servizi di mobilità (host fissi). Il protocollo "IP-Mobile" consente di superare questo vincolo, facendo sì che nodi mobili, con preassegnati indirizzi IP, possano continuare a comunicare al variare del proprio "Current Point of attachment" senza modificare il proprio indirizzo.

Come sappiamo un indirizzo IPv6 indica in modo univoco un nodo e la sua locazione. Con gli indirizzi Mobile Ipv6 identifichiamo non solo la locazione ma anche l'identità. Tali indirizzi sono composti da 128 bit di cui 64 bit sono usati per indicare la locazione e i restanti 64 specificano l'identità. La struttura degli indirizzi Mobile Ipv6 è la seguente:



Un nodo mobile è sempre raggiungibile tramite il suo *Home Address* ovvero un indirizzo IPv6 che viene assegnato al nodo quando si trova nella sua *Home Network* e questo permette di raggiungere il nodod anche non è nella sua *Home Network* , ma in un altra sotto-rete , usando un meccanismo del tutto trasparente.

I nodi mobili all'interno della propria HN adottano un *Home Agent*: un router IPv6 direttamente collegato alla

Home Network responsabile dell'intercettazione e dell'inoltro dei pacchetti IPv6 ai nodi mobili anche (e sopratutto) quando questi ultimi sono assenti dalla HN.

Quando un nodo mobile IPv6 è connesso alla relativa HN funziona come come un qualsiasi altro nodo ovvero è raggiungibile direttamente tramite il suo *Home Address.* Quando invece l'utente si sposta avviene un processo tramite il quale al nodo viene riconfigurato un nuovo IPv6 che prende il nome di *Care-of address* realizzato unendo l'attuale prefisso di sotto-rete con il MAC *address* del nodo. Il nodo possiede cosi due indirizzi l'*Home-Address* usato nella sua *Home Network* e il *Care-of Adress* usato invece quando il nodo è in una sotto-rette ospite e che inoltre ha una durata (*lifetime)* decisa dall'Home Agent. Tutti gli altri nodi che comunicano con il nodo mobile sono detti *nodi corrispondenti*.

4.3 Secure Binding Updates

L'associazione tra l'*Home Address* del nodo mobile e il *Care-of Address* è chiamata *binding* per il nodo mobile.

Per fare in modo che i pacchetti IPv6 destinati all'Home Address raggiungano efficientemente la corretta posizione, le informazioni di routing (bindings) relative all'Home Address devono essere aggiornate sia presso l'Home Agent che in tutti gli eventuali nodi corrispondenti con il nodo mobile. MIPv6 fornisce questa funzionalità tramite l'introduzione di una "binding cache" memorizzata in ogni nodo ed un sistema di messaggi (Binding Messages) . Tale cache viene ovviamente aggiornata usando un meccanismo detto Binding Update (BU).

Tali messaggi vengono trasmessi usando l'Home Agent come sender e il nodo mobile comunica con questo tramite una comunicazione sicura (esempio facendo uso di un tunnel).Risulta chiaro quindi come tali aggiornamenti *binding* debbano essere fatti in maniera sicura infatti se un BU non viene verificato un utente può corrompere la *binding cache* e creare scompiglio non solo nella rete mobile, ma anche in quella collegata. Una prima idea può essere quella di usare il protocollo IPSEC ma tale non presenta un applicabilità a reti mobile. É necessario quindi definire una catena di fiducia tra il nodo mobile i corrispondenti nodi in assenza di un protocollo generale tipo PKI per internet.

E' necessario quindi uno strumento per rendere sicuri i *binding update* e in Mobile IPv6 questo viene fatto tramite due mezzi:

1) proteggendo i messaggi di binding tra Mobile Network e Home Agent tramite l'uso di IPSEC (che richiede una mutua autenticazione)
2) tra Mobile Network e Corrisponden Node usando un protocollo di tipo *return routability* che assicura quest'ultimo che chi ha inviato il BU sia chi dichiara di essere.

Il sistema utilizzato per rendere sicura la comunicazione prende il nome di Return Routability

In questo protocollo il nodo mobile per prima cosa invia due *INIT MESSAGE* ai nodi corrispondenti, uno detto *Home Test Init* inviato tramite l'Home Agent e l'altro detto C*are-of test init* inviato invece direttamente ai nodi corrispondenti. I nodi corrispondenti risponderanno ciascuno in modo indipendente ad entrambe le richieste inviando un messaggio detto HOME TEST contenente una chiave keygen K0 e un indice i (nonce) e questo spedito tramite la home address del nodo. Quindi viene inviato anche un messaggio in maniera diretta al nodo detto CARE OF TEST contenente una chiave keygene K1 e il nonce j.

Il nodo usa tali informazioni per computare una chiave segreta usando la chiave della HOME TEST K0 e quella del CARE OF TEST K1, ovvero genera una chiave cosi posta :

K_{bm}= SHA1(home keygene token || care-of keygene token),

e genera poi un Binding Update (BU) e lo invia usando tale chiave K_{bm} per firmare il MAC (Message

iAuthentication Code che autentica il nodo) e inviando anche i nonce inviatagli dai nodi corrispondenti.

BU(MAC($K_{bm,}$),i,j).

Quindi i nodi CN ricevuto il BU possono aprirlo usando le chiavi e inviano un ackwnolodgment come conferma di ricezione (Binding Ackwnolodgment).

Questo protocollo può essere vulnerabile ad attacchi mirati a intercettare entrambe le comunicazioni che passano non via etere verso i CN e recuperare ad esempio le chiavi con cui cifrare il BU, ma come detto la comunicazione non via etere può essere protetta con Ipsec. Per essere resistente ad attacchi di tipo DoS è necessario che i nodi corrispondenti non ricordino le chiavi K0 e K1 o meglio ciascun nodo facendo uso di una chiave segreta detta Kcn determina le proprie chiavi K0 e K1. Tale chiave è segreta nel nodo e non viene condivisa con nessun'altra entità.

Ciascun nodo poi genera un nonce nuovo a intervalli regolari e genera le chiavi usando i primi 64 bit del MAC. Si hanno quindi le chiavi così generate:

K_0:=HMAC_SHA1(K_{cn}, HoA || nonce[i] | $0)_{64}$

K_1:=HMAC_SHA1(K_{cn}, CoA || nonce[j] | $1)_{64}$

dove K_{cn} è appunto la chiave segreta e HMAC_SHA1 è la funzione di Hash e in seguito verranno distrutte per generarne delle altre.

Un protocollo così fatto dove più messaggi sono inviati in replica a un messaggio ricevuto , può aumentare il rischio di attacchi DoS e per questo motivo che la richiesta di BU è divisa in due parti ovvero il nodo mobile può inviare l'indirizzo home e l'indirizzo care-of in un unico messaggio, ma la risposta dai nodi corrispondenti avviene su due messaggi.

5 WLAN Security

WLAN meglio nota come wireless LAN ovvero Wireless Local Area Network è una tecnologia per le reti senza filo ed è definita nello IEEE 802.11.

In una Wlan viene utilizzata una tecnologia di radio frequenza RF per la trasmissione e la ricezione dei dati, minimizzando la necessità di connessioni via cavo (wired).

La sicurezza fondamentale di questa tecnologia riguarda essenzialmente l' accesso alla rete , l'integrità e la confidenzialità dei dati trasmessi che devono essere protetti. Per raggiungere tali obiettivi sono stati definiti degli algoritmi crittografici per la gestione delle chiavi, nonché un controllo degli accessi alla rete. Un WLAN non protetta infatti permette ad un attaccante di utilizzare una connessione a internet liberamente dandoli anche la possibilità di sviluppare un attacco alla rete o alla vittima stessa.

Le reti WLAN in genere possono operare secondo due modalità , nella modalità infastructure i terminali mobile si collegano alla rete tramite un access point , nella modalità ad hoc i terminali comunicano direttamente. Noi ci occuperemo della prima modalità e in particolare del controllo degli accessi all'access point. Elemento fondamentale delle WLAN è l'access point , ovvero un apparecchio che consente ai terminali mobili di collegarsi alla rete.

Ogni access point possiede un identificativo detto SSID (Service Set Identifier) e in una WLAN aperta (libera) non vi sono restrizioni su chi può accedere all'access point , quindi per un utente basterà collegarsi all'access point (AP) per accedere alla rete. Notiamo che una WLAN aperta non significa necessariamente che la rete non sia protetta in quanto i meccanismi di protezione possono essere implementati in altri livelli protocollari.

Un primo controllo sull'accesso a una WLAN può essere quello di configurare gli access point in modo da non fornire il prorpio SSID (il nome con cui una rete Wi-Fi si presenta agli utenti) in maniera broadcast, ma richiedere che i clienti che vogliano comunicare con esso, conoscano l' SSID. L'SSID rappresenta quindi il segreto necessario per accedere alla rete in quanto la rete c'è ma gli utenti non la vedono. Non si tratta però di

una vera misura di sicurezza in quanto la rete è comunque individuabile perchè il valore dell'SSID (che sono dei caratteri ASCII) è presente nei messaggi trasmessi tra gli AP e i client e può quindi essere intercettato tramite opportuni programmi anche se l'SSID è nascosto.

Un altro metodo è quello di far si che l'AP accetti connessioni solo da utenti con un certo MAC (medium access controll ovvero l'indirizzo fisico della rete del client che si vuole colllegare) , riconosciuto come valido dall'AP, ma anche questo metodo non è sicuro in quanto un attaccante può determinare un valido MAC intercettando le connessioni tra device legittime e l'Hot Spot eseguendo uno spoofing degli indirizzi MAC.

Un'altra tecnica di accesso è quella definita UAM (Universal Access Meccanism) che funziona cosi:

un client si suppone abbia un browser web e quando richiede l'accesso alla rete dopo essersi collegato a un access point , questi gli assegna tramite DHCP un indirizzo IP dinamico. Quando il client avvia il browser e richiede una connessione http , questa viene intercettata e la connessione è reindirizzata a una connessione https verso una pagina in cui l'utente deve inserire nome utente e password che vengono verificate dall'access point con quelle memorizzate su un RADIUS server, se coincidono si ottiene l'autenticazione e l'utente può accedere alla rete.

5.1 WEP

Il protocollo WEP (Wireless Equivalent Privacy) è stato definito nell'IEEE 802.11 ed è uno standard usato per definire la confidenzialità e l'integrità dei dati passati tra un terminale mobile e un access point e per autenticare i terminali mobile alla rete.

L'autenticazione si basa su una chiave condivisa e tale chiave WEP a 40 bit condivisa viene salvata su ogni device che debba accedere alla rete e su tutti gli acess point che consentono l'accesso alla rete. Questo protocollo va bene se la rete è piccola come le reti domestiche anche perché la chiave spesso è inserita a mano negli AP e non vi è un protocollo do gestione.

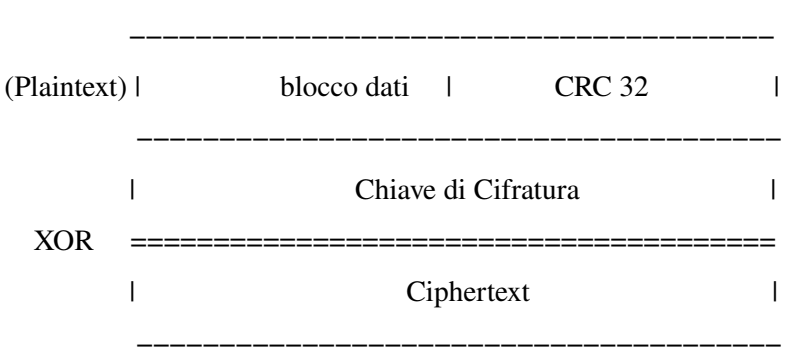
WEP usa uno stream cipher per eseguire la criptazione dei dati trasmessi tra AP e i nodi L'algoritmo utilizzato è l'RC4, uno Stream Cipher ideato da Ron Rivest dell'RSA Security. L'algoritmo di per se è sicuro, veloce e abbastanza leggero da implementare. Tale procede cosi :

Alla chiave (segreta) WEP di 40 o 104 bit viene aggiunto un vettore di inizializzazione (IV) di 24 bit in modo da formare una chiave intermedia di 64 o 128 bit. L'IV è un numero che viene generato dall'AccessPoint o dalla Stazione, spesso è un registro che viene incrementato di 1 ogni volta che viene utilizzato. In questo modo si possono generare 2^24 (quasi 17 milioni) chiavi intermedie. La chiave intermedia è l'input dell'algoritmo RC4 che genera una Chiave di Cifratura (o Stream) di lunghezza fissa ovvero:

Chiave_Intermedia = Chiave_WEP ∪ IV

Chiave_Cifratura = RC4(Chiave_Intermedia)

Contemporaneamente i dati da cifrare vengono divisi in blocchi di lunghezza fissa, e di ogni blocco viene calcolata una checksum CRC a 32 bit che viene aggiunta in coda al blocco. Il blocco di dati più la checksum forma il Plaintext ed ha la stessa lunghezza della Chiave di Cifratura . Nell'ultimo passaggio si esegue un XOR del Plaintext con la chiave di cifratura per ottenere il CipherText o messaggio cifrato



Il procedimento di decrittazione è l'esatto opposto: mettendo insieme la chiave (segreta) WEP presente nel device e l'IV ottenuto dal pacchetto stesso, utilizzando RC4 si genera la stessa Chiave di Cifratura. Facendo l'XOR del Ciphertext con la Chiave di Cifratura, che serve quindi anche per de−cifrare, si ottiene il Plaintext, si controlla se la checksum CRC−32 è corretta e nel caso si accetta il pacchetto. Bisogna notare che l'IV è inviato in chiaro nel pacchetto, e non potrebbe essere altrimenti poiché il ricevente in caso contrario non potrebbe calcolarsi la Chiave di (de−) Cifratura. D'altronde la sicurezza di RC4 garantisce che un attaccante in possesso solo di un IV e del corrispondente Ciphertext, non è in grado di risalire alla Chiave di Cifratura.

PROBLEMATICHE DEL WEP

Purtroppo WEP soffre di vari problemi in primo luogo l'IV è un numero a 24 bit, e quindi permette di creare solo circa 17 milioni di chiavi intermedie. Ipotizzando di inviare pacchetti di 1500Bytes a 11Mbps, ognuno con un IV diverso, bastano poco più di 5 ore per esaurire gli IV. In pratica però ci vuole molto meno, poiché ad esempio in caso di errori di trasmissione (collisioni ecc.) il protocollo WEP richiede la reinizializzazione degli IV. Se poi gli IV fossero dati in modo casuale, ci vorrebbe ancora meno per avere una ripetizione. Inoltre non è necessario conoscere completamente un Plaintext o fare un known plaintext attack, infatti sfruttando gli header dei pacchetti, che sono spesso facilmente indovinabili, ed i pacchetti tipo ARP, IP, SNAP ecc. che spesso si ripetono nella rete, è possibile ottenere sufficienti informazioni per ricostruire la Chiave di Cifratura. Il tutto è così semplice, che esistono programmi come Airsnort e Wepcrack che rendono del tutto automatico . Un altro problema, veniale a paragone del precedente, che è stato trovato in WEP è nell'utilizzo di CRC−32. CRC, Cyclical Redundacy Check, è un algoritmo di checksum che permette di calcolare un numero di lunghezza fissa, 32 bit in questo caso, caratteristico del pacchetto inviato. La checksum viene calcolata prima dell'invio e della criptazione dei dati, ed inserita nel pacchetto; all'arrivo viene ricalcolata e confrontata con quella presente nel pacchetto. Se vi è una differenza vuol dire che il pacchetto è stato modificato in qualche modo, e quindi viene scartato. Il problema principale con CRC−32 è che è una checksum lineare, ed è stato trovato il modo di modificare un bit nella parte dati del pacchetto ed un bit nella checksum in modo che i nuovi dati corrispondano alla nuova checksum, il tutto all'interno del pacchetto crittato con WEP .

Esempi di attacchi dovuti a queste debolezze sono:

Known PlainText Attack (sistema immagini)
Se facciamo lo XOR di due pacchetti cifrati con gli stessi IV e Wep Key si ottiene un risultato interessante:

$$C1 \oplus C2 = (P1 \oplus KeyStream) \oplus (P2 \oplus KeyStream) = P1 \oplus P2$$

Questo significa che dati due pacchetti cifrati, è possibile ottenere lo XOR dei corrispondenti pacchetti in chiaro. Di conseguenza se un attaccante conoscesse uno dei due PlainText, potrebbe conoscere il contenuto dell'altro in questo modo:

$$P1 \oplus (C1 \oplus C2) = P1 \oplus (P1 \oplus P2) = P2$$

Inoltre, conoscendo un PlainText e il relativo Testo Cifrato, è possibile ottenere il KeyStrem facendone lo XOR. Conoscendo alcuni KeyStream e i relativi vettori d'inizializzazione IV, è anche possibile sfruttare una debolezza dell'algoritmo RC4 e ottenere la Wep Key[1] utilizzando la criptoanalisi differenziale. Saranno ora esaminati alcuni metodi per ottenere una valida coppia PlainText e Testo Cifrato.

Packet Injection
Una conseguenza della seconda proprietà della checksum è che la stringa di controllo può essere calcolata anche da un avversario che possiede una valida coppia PlainText/Testo Cifrato, ma che non conosce la Wep Key. Infatti è noto che:

$$P1 \oplus C1 = KeyStream.$$

Si conosce anche l'IV associato al Testo Cifrato C1 , di conseguenza è sufficiente scegliere un PlainText qualsiasi, eseguire lo XOR con il Keystream ed ottenere un valido Testo Cifrato che l'Access Point considererà valido a tutti gli effetti. Questo attacco è noto come Packet Injection in quanto permette di inviare pacchetti di qualsiasi tipo nella Wireless Lan attaccata.

5.3 WPA

Come si è visto il protocollo WEP ha fallito totalmente nel cercare di raggiungere i suoi obiettivi sulla sicurezza ,venne cosi definito un nuovo standard denominato Wifi Protected Access (WPA) con il principale scopo di ridefinire totalmente gli aspetti di sicurezza delle reti WLAN.

Tra le migliorie furono poste ad esempio nuove tecniche per l'autenticazione dei client alla rete e per stabilire una chiave crittografica temporanea , questo usando ad esempio il protocollo EAP (Extensible Authentication Protocoll) che supporta vari metodi di autenticazione basati su token cards, Kerberos, password temporanee, ecc...è un protocollo di autenticazione utilizzato spesso sugli access point e nelle connessioni PPP. L'utilizzo di EAP all'interno di una rete wireless, ad esempio, prevede che non sia l'access point ad autenticare il client: esso redirige la richiesta di autenticazione avanzata dal client ad uno specifico server, configurato per questo scopo come un RADIUS.

Per aumentare la protezione dell'integrità dei dati inoltre il CRC-32 fu sostituito da un messaggio di integrità MIC e la lunghezza dell'IV fu aumentata a 48 bit.

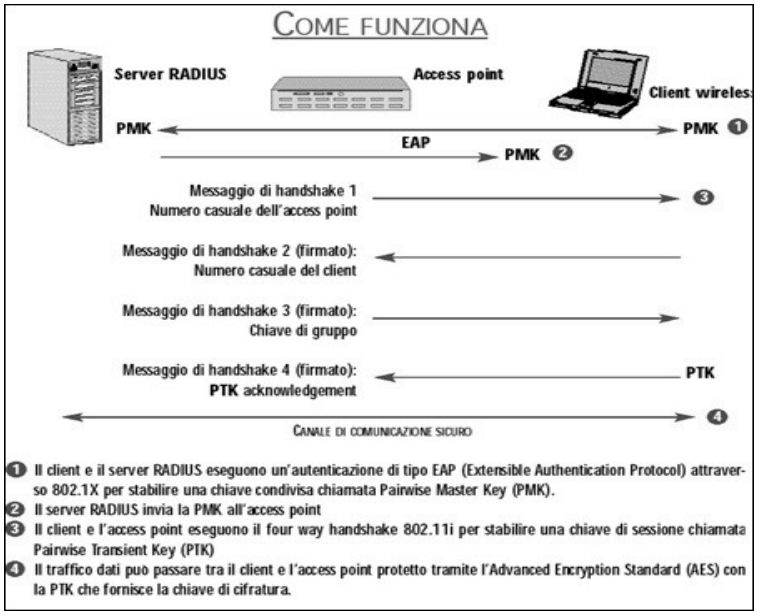
Il meccanismo di autenticazione è detto *four-way handshake* che opera così :

All'inizio l'access point (AP) deve autenticarsi e la chiave di sessione utilizzata per cifrare i messaggi deve ancora essere calcolata. In primo luogo viene stabilita, tra la stazione wireless (STA) e l'AP, una chiave chiamata Pairwise Master Key (PMK). Questa chiave è generata tipicamente durante il procedimento di autenticazione dell'utente verso un server RADIUS (o di altro tipo) sfruttando l'EAP. Sia il client che il server RADIUS ottengono chiavi identiche, e il secondo restituisce la chiave all'AP. A questo punto STA e AP si scambiano una sequenza di quattro messaggi, nell'ambito dello schema "four-way handshake".

Per prima cosa si trasmette all'access point una chiave temporanea PTK (Pairwise Transient Key). LA PTK è generata concatenando PMK, una nonce dell'AP, una nonce di STA ed infine l'indirizzo MAC di STA e dell'AP. Il prodotto di questa concatenzione viene inviato ad una funzione crittografica di hash. La PTK è a sua volta suddivisa in più chiavi: una per firmare i messaggi "four-way handshake"; una per rendere sicuri i pacchetti dati trasmessi tra STA e AP; una per cifrare presso la stazione, e durante la fase di four-way handshake, la "group key". Quest'ultima consente all'AP di trasmettere un pacchetto multicast a tutte le stazioni, piuttosto che inviare un pacchetto separato e cifrato a ciascuna di esse.

Nel corso della fase di four-way handshake, la stazione e l'access point negoziano, inoltre, il tipo di cifratura che deve essere impiegato per la connessione dati. Vengono quindi negoziati due algoritmi di cifratura: quello "pairwise" è utilizzato per la trasmissione unicast dei dati tra la stazione e l'access point mentre quello "group" è per la trasmissione broadcast/multicast del traffico dall'access point a più stazioni.

Una miglioria ulteriore è stata posta con l'implementazione del protocollo WPA2 che prevede ad esempio l'uso di AES come stream cipher al posto di RC4.



Possibili debolezze derivano dal fatto che quando WPA lavora in modalità personal una chiave unica, la Pre-Shared Key(PSK) viene utilizzata da tutti i client. Si può però avere che ogni stazione abbia la propria chiave generata a partire dalla PSK e legata all' indirizzo MAC della stazione stessa, oppure la chiave è la PSK stessa. La PSK è una chiave a 256 bit o una password da 8 a 63 caratteri. Accade che se la PSK utilizzata è a 256 bit, questa vine utilizzata direttamente come PMK, altrimenti se è di lunghezza minore la PMK viene derivata attraverso una funzione hash che prende in input la password, il nome della rete wireless, la lunghezza dello stesso e restituisce un hash di 256 bit. La PTK invece è generata a partire dalla PMK utilizzando i due indirizzi MAC e le due nonces che vengono scambiate nei primi due pacchetti durante il processo di four-way handshake e serve inoltre sia per firmare i messaggi durante questo processo, che per generare le chiavi successive del TKIP.

Quindi conoscendo la PSK è possibile ricavare la PTK e tutta la gerarchia delle chiavi. Un utente che già conosce la PSK perchè magari è autorizzato ad accedere alla rete, può calcolare la chiave utilizzata da tutte le altre stazioni wireless presenti semplicemente “sniffando” i pacchetti del four-way handshake che contengono le nonces. Quindi anche se le chiavi sono diverse per ogni stazione, all'interno della rete non c'è nulla di privato. Se invece una stazione non conosce la PSK, può romperla mediante un attacco offline.

La PTK è usata per produrre l'hash dei messaggi durante il four-way handshake ed esiste una lunga lista di attachi offline a dizionario contro gli hash. E' quindi possibile modificare uno di questi programmi per prendere in input i dati ottenuti catturati durante il processo di autenticazione per realizzare l'attacco.

6 Bluetooth (cenni)

Per terminare la trattazione sulla sicurezza delle reti mobile poniamo un piccolo accenno alla tecnologia Bluetooth. Tale è uno standard per reti Wireless nella modalità ad-hoc , quindi una comunicazione diretta tra i terminali senza uso di access-point.

Inizialmente fu inventata per una ristretto campo d'azione (circa 10 m) e per mettere in comunicazione i vari dispositivi di un PC come tastiere o mouse o altre periferiche formando cosi una Personal Area Netwok e essendo una rete ad-hoc non richiede una sofisticata infrastruttura di rete.

La sicurezza di una comunicazione tra due device si può ottenere ad esempio usando un codice PIN tra in comune tra i due device , ovvero un dispositivo se vuole comunicare con un altro deve avere un impostato in comune con quel dato dispositivo PIN.

Pe rendere sicura tale comunicazione viene usata una chiave di collegamento a 128 bit derivata dal PIN usata per le successive comunicazioni e l'autenticazione avviene usando un protocollo del tipo challenge-response , come nel sistema GSM.

Nel Novembre del 2003 Ben e Adam Laurie scoprirono delle falle di sicurezza nel protocollo Bluetooth. Queste falle consentivano l'accesso a dati personali da parte di un estraneo. È da segnalare che i difetti riguardavano alcune pessime implementazioni del protocollo e non affliggevano tutti i dispositivi Bluetooth.

In un esperimento successivo, Martin Herfurt ha dimostrato durante il CeBIT quanto era importante il problema della sicurezza.

Nell'agosto del 2004 durante il world-record-setting experiment è stato dimostrato che è possibile intercettare il segnale Bluetooth anche a un miglio di distanza utilizzando un'antenna direzionale ad elevato guadagno e bassissima distorsione. Questo estende significativamente il possibile raggio di azione di un potenziale aggressore.

Bluetooth utilizza l'algoritmo SAFER+ (Secure And Fast Encryption Routine) per autenticare i dispositivi e per generare la chiave utilizzata per cifrare i dati.

Quando si trova in modalità "rilevabile", il telefono cellulare Bluetooth o il PDA invia un segnale che indica la disponibilità ad "abbinarsi" ad un altro dispositivo Bluetooth per scambiare dati. Tuttavia, un utente malintenzionato che individua questo segnale può provare ad abbinarsi al dispositivo dell'utente e rubarne il codice PIN. Mentre questi rimane del tutto ignaro, l'utente malintenzionato, con il PIN rubato, può effettuare varie operazioni come sottrarre informazioni , o inviare messaggi o dei virus per il dispositivo. La sicurezza dei dispositivi è garantita da cinque elementi:

• **Indirizzo BT_ADDR:** L'indirizzo fisico del singolo dispositivo; ogni indirizzo è unico poichè assegnato dall' IEEE e collegabile al produttore che ha realizzato l'apparecchio. L'indirizzo è un campo di 48 bit (esempio: 00:0A:D9:62:12:36) di cui i primi 24 bit sono legati alla casa produttrice (in questo caso Sony Ericsson). Anche per la tecnologia Bluetooth è possibile, su alcuni dispositivi, modificare questo valore cambiando "l'identità" del dispositivo.

- **Chiave di cifratura** (8-128 bit) utilizzando l'algoritmo SAFER+
- **Chiave di collegamento** (128 bit)
- **Numeri pseudocasuali** (128 bit)
- **Vari algoritmi per la generazione delle chiavi**

Riassumiamo infine brevemente i principali attacchi:

Bluejacking: Il nome del dispositivo è un campo di testo che può contenere una stringa maggiore o uguale di 248 caratteri (ove possibile). In tal modo si sa chi ha il bluetooth attivo. L'utente inesperto ricevendo, ad esempio, un messaggio di questo tipo: "Problemi alla rete, digita 1234 per associare il telefono alla cella" o "Vodafone ti regala una suoneria..digita 1234 per proseguire" potrebbe essere tratto in inganno, facendo diventare trusted un dispositivo sconosciuto che quindi acquisirebbe tutti i privilegi necessari a compromettere i dati e le comunicazioni.

"Discovery mode" abuse: Molti dispositivi permettono varie opzioni per il bluetooth come visibile scosto, spento. Un utente mettendosi nascosto può pensare di sfuggire a un attacco, in realtà ci sono programmi che permettono di individuare i dispositivi nascosti come RedFang un programma che esegue un brute-force sugli ultimi 24 bit dell'indirizzo del dispositivo per rintracciarlo.

"Blue-snarf e blue-bag: il primo consiste nello sfrutatre il servizio OBEX per l'invio di cartoline elettroniche e sfruttando bug del sistema si permette al telefono non solo la ricezione ma anche l'invio di dati, il secondo obbliga il cellulare a telefonare a un numero e sfruttando bug del sistema si può accedere ai suoi dati.

Come suggerimento per aumentare la sicurezza Bluetooth l'utente può adottare alcune semplici precauzioni che è bene ricordare:

• Scegliere codici PIN non banali e lunghi.I codici composti da cinque o più cifre sono più difficili da indovinare.

• Evitare il pairing tra dispositivi Bluetooth in ambienti affollati o poco sicuri

• Utilizzare il dispositivo in modalità nascosta o invisibile per

• Evitare di memorizzare dati riservati, come il codice fiscale, il numero di carta di credito e le password, sui dispositivi wireless.

• Installare un buon antivirus.

RIFERIMENTI

Www.dia.unisa.it/~ads/corso-security/www/corso-9900/a5/index.htm

www.gsm-security.net

www.haccanada.com/blackcrawl/cell/gsm/gsm-security/gsm-security.htm

http://it.wikipedia.org/wiki/Global_System_for_Mobile_Comunication.html

http://user.libero.it/sandry/Mappa.html

http://securytech/home.unix.org/Projects_EISE

http://student.grm.hia.no/master/IKT01/ikt6400/jrdohm99/thesisumtSAKA.pdf

http://it.wikipedia.org/wiki/Universal_Mobile_Telecomunication_System

www.6net.org/events/workshop/-2005/lucetti.pdf

www.ippar.unict.it/wikippari/wiki/index.php?page=wep&wpa

www.ippari.unict.it/infapp/didattica/appunti/siurezza%20/dei%20sistemi%20informatici%202/tesine/wpa.pdf

www.geocities.com/boss84x/informati/tesina_final.pdf

http://sicurezza.html.it/articoli/leggi/1650/id-sicurezza-nelle-comunicazioni-bluetooth/2/