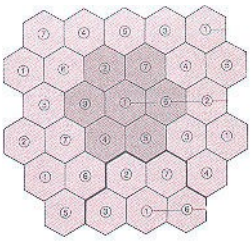
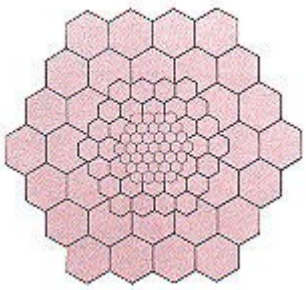
- **Funzionamento reti cellulari**

Ogni rete cellulare e' costituita da un numero variabile di celle che permettono la copertura radio-elettrica e il collegamento tra i terminali mobili e la rete telefonica fissa. Il numero delle celle e la loro grandezza dipende dalla quantita' di traffico (e quindi dal numero di terminali mobili) presenti in una data zona. Nelle citta' il numero delle celle e' molto alto e la loro grandezza e' molto ridotta. Lo schema seguente rappresenta uno schema classico di celle in una rete cellulare cittadina, la grandezza delle celle dipende dalla tipo di traffico presente in ogni zona.



Rete cellulare classica



Rete cellulare cittadina

- **Analisi Algoritmo A5**

L'algoritmo utilizzato per crittare i pacchetti di dati contenenti la nostra voce viene indicato con la sigla A5. Non essendo un prodotto di pubblico dominio, i suoi sorgenti di sviluppo non sono liberamente reperibili. Già solo questo dato dovrebbe indurci a una maggiore prudenza e a legittimi dubbi sull'affidabilità dell'algoritmo stesso.La nascita dell'A5 non è espressamente legata alla rete GSM. L'algoritmo venne adottato dopo una lunga battaglia tra i vari paesi appartenenti al consorzio paneuropeo da cui nacque la necessità di creare un sistema di telefonia digitale sicuro e standardizzato. Nella competizione vinse l'idea di una rete non invulnerabile e per la rete GSM venne adottata una versione modificata dell'A5, chiamata AX. Questo sistema si basa su un codificatore di tipo str eam ci pher (utilizzato per cifrare un ciclo continuo di bit da trasmettere) che utilizza secondo i parametri ufficiali ETSI una chiave di cifratura di 64 bit per codificare i 114 bit di ogni burst (pacchetto di dati) che viene trasmesso da base a unità mobile.Secondo l'esperto di crittografia inglese Ross Anderson l'ultimo dato non é reale e la chiave effettiva sarebbe di soli 5 byte (40 bit). Ciò rende fattibile la ricerca della chiave di partenza avvalendosi di soli pochi giorni di calcolo di una workstation o di un potente personal computer. Secondo Anderson sa- rebbe molto facile realizzare dei chip progettati apposta per realizzare un banale attacco a 2^40 combinazioni, che permetterebbero la nascita di un fantastico cracker di A5.Nel giugno del 1994 una possibile implementazione dell'A5X è stata diffusa su Internet e vari sono i gruppi che stanno lavorando per la realizzazione di un veloce e funzionale generatore di chiavi. Sempre nel giugno 1994 si doveva tenere all'IEE di Londra un incontro organizzato dal professor Simon Sherpherd della Bradford University sui problemi di sicurezza degli algoritmi stream cipher e soprattutto dell'A5. Incredibilmente il GCHQ (il servizio inglese di intelligence) riuscì a far saltare la presentazione.Un ulteriore segnale della effettiva non sicurezza di questo sistema lo possiamo apprendere da un documento scritto da Marcello Scatà e Lorenza Romano (disponibile liberamente in rete) della facoltà di Ingegneria Informatica di Padova, su cui troviamo il seguente passaggio:
"Supponiamo che effettuare una ricerca esaustiva di tutte le possibili chia vi sia il metodo più efficiente per decifrare un messaggio cifrato. Possiamo allora considerare la dimensione della chiave come una misura dell'affidabilità di un algoritmo di crittografazione. Se assumiamo una cracking ma chi ne capace di un milione di crittografazioni al secondo, otteniamo i seguenti risultati:

Dimensione chiave in Bit	32	40	56	64	128
Tempo richiesto per verificare tutte le possibili	1,19 Ore	12,7 Giorni	2.291 Anni	584.542 Anni	10,8 * 10^25 Anni

chiavi					

Nel valutare l'affidabilità di un algoritmo di crittografazione deve essere perciò considerata la "durata" delle informazioni che devono essere protette. Assumendo ad esempio che l'algoritmo A5 utilizzato nel sistema GSM abbia, come sembra, una effettiva chiave di 40 bit (e non 64 bit), fornisce una adeguata protezione per informazioni che hanno un tempo di vita breve. È opinione comune che le conversazioni telefoniche cellulari abbiano un tempo di vita utile dell'ordine di qualche settimana".

In che cosa consiste il Phreaking?

In poche parole consiste nella manomissione più o meno visibile e identificabile di sistemi telefonici fissi o mobili.

Come ogni apparecchio elettronico, anche i telefoni (cabine telefoniche comprese) si basano prevalentemente su software e sistemi di controllo computerizzati.

Questo permette a chi è del mestiere di inserirsi e modificarli facilmente a proprio piacimento, magari per scroccare una telefonata o per ricaricarsi la scheda telefonica (o il cellulare perchè no).

In principio, quando ancora giravano copiosi gli stupendi gettoni telefonici (quelli color rame per intenderci) le cabine erano oggetto di intensi attacchi soprattutto per ricaricare il credito delle schede telefoniche.

Infatti il funzionamento delle schede telefoniche è facilmente riassumibile cosi. Su ogni carta che viene emessa nel mercato viene assegnato un codice numerico (visibile nella scheda) composto da due parti,

-una che identifica il credito della scheda (esempio: la carta da 5000 ha un codice 01, quella da 10.000 02 ecc) ed è standard;

-l'altra che identifica la scheda è un codice univoco (ovvero unico).

Quando la scheda viene inserita nella cabina telefonica, un apparecchio legge il codice e dà la possibilità di utilizzare il credito contenuto.

Teoricamente, se fossimo in grado di generarci i codici, potremmo crearci schede telefoniche ogni qualvolta ne avessimo bisogno.

Non sono stati risparmiati nemmeno i cellulari,anzi, questi ultimi, utilizzando massicciamente software per il funzionamento, hanno subito intensi attacchi, soprattutto in questi ultimi anni. Non solo riuscendo a telefonare gratuitamente o scroccando gli Sms, ma anche clonando i cellulari, permettendo di telefonare utilizzando il credito di altri utenti (operazione nemmeno troppo difficile avendo un minimo di conoscenze di base).

La parola Phreaking è l'unione delle due Phone e Hacking. Il Phreaking è un'arte il cui momento di massimo splendore si ebbe agli inizi degli anni '90, e consisteva, e consiste tutt'oggi, nel poter fottere tutta la telefonia in generale, o meglio effettuare chiamate gratuite da cabine telefoniche, clonare cellulari E-TACS, modificare le memorie dei cellulari, intercettare chiamate, fare in modo che la telefonata non sia tracciata, modificare i dati contenuti nelle tessere magnetiche di ultima generazione (quelle con il "ragnetto"), mandare Free-SMS, eccetera.

In poche parole è l'arte di hackerare il telefono e tutto ciò che lo riguarda, quindi le telecomunicazioni in genere. Le possibilità nel mondo delle telecomunicazioni sono praticamente infinite... e, chiusa una strada se ne trova subito un'altra. Purtoppo in italia il phreaking non è così diffuso come in America, ma si possono lo stesso fare interessanti scoperte.

Bisogna dire che questo non è decisamente un periodo d'oro per il phreaking, che qui in Italia ha visto la sua golden Age nei primi anni 90, quando per sbafare le telefonate c'era solo l'imbarazzo della scelta, ora l'unico fenomeno eclatante sembra la comparsa dei famosi 'green' per la connessione ad Internet.

Adesso la Telecom ha affiliato le unghie e l'antica arte del Phreaking rischia di scomparire.

Si intravede una luce nella liberalizzazione del settore delle telecomunicazioni, ma resta ancora tutto da vedere. I bug delle cabine vengono corretti man mano che vengono scoperti e così al phreaker non resta altro che la vandalica soluzione di portarsi a casa un rotor per souvenir, per poi scoprire che non è capace ad interfacciarlo al PC.

Ma cosa sono i Rotor?

Allora, ora vi spiego cosa so io dei rotor: I fili che arrivano al rotor sono 4, e non 2 come si potrebbe supporre: due sono per la voce, gli altri sono per lo scambio dati del telefono con la sua centrale. (se ti connetti ai due fili voce con una beige box (lineman handset) il telefono rileva tale operazione, e la linea viene bloccata.).

Il rotor è alimentato dall'esterno, dalla tensione di rete.

Il lettore di tessere è un altro capolavoro di ingegneria: tre testine di lettura e due di cancellazione situate nella parte posteriore dell'apparato, la tessera che viene mossa da nastri, e la sua posizione è controllata da fotoaccoppiatori (praticamente non li puoi fottere).

QUALCHE CENNO SULLE SCHEDE MAGNETICHE.

Le carte magnetiche si dividono in due gruppi: Le carte Iso-standard e quelle band-origin.

Delle carte band-origin (carte telefoniche da 5/10m lire (ma ora si deve parlare in EURO), viacard, airport free, Go bank, Electronic money) e' inutile parlare ...

possiedono codici magnetici particolarissimi e leggibili solo da reader speciali non in vendita al pubblico.

Le carte telefoniche da 5/10000 lire hanno perfino una quarta traccia magnetica di protezione oltre alle tre usuali che fuoriesce dalle misure standard per cui oltre al lettore speciale serve anche un particolare decodificatore URMET che la URMET di Roma appunto non vi venderebbe nemmeno se vi presentaste travestiti da monsignore col passaporto rosso!

C'e' pero' un dato di fatto: ogni cabina telefonica possiede un lettore-scrittore della URMET!

Pero' (almeno nelle cabine un po' vecchiotte) e' ATTACCATO al telefono!!!

- FUNZIONAMENTO DI UNA COMUNICAZIONE TELEFONICA

Quando una chiamata avviene tra settori diversi, ovviamente nasce un dialogo tra

la centrale locale e la centrale remota.

Se, semplificando, supponiamo che le centrali siano solamente 2, una di partenza ed una di arrivo, la chiamata telefonica viaggia su doppino analogico fino alla centrale locale, in pacchetto PCM digitale (partizione di tempo) tra le due centrali e di nuovo in doppino dalla remota al terminale.

Un utente normale puo' inviare alla propria centrale i 12 toni (con cui poi l' SW di

centrale potra' fare un numero arbitrario di funzioni, di cui quella piu' semplice e'

selezionare un altro utente) piu' il suo stato analogico di commutazione. (toni dtmf).

A loro volta, le centrali hanno il proprio sistema di dialogo. Questo deve comprendere, per logica, almeno i 12 toni suddetti, affinche' l'informazione sul destinatario da selezionare possa essere trasferita alla remota. Inoltre le centrali hanno bisogno di altri toni supplementari... e' intuitivo che la centrale non puo' inviare in modo analogico lo stato di commutazione per 5000 Km, quindi rappresenta la stessa info con toni.

Questi toni in piu' esprimono informazioni tra cui inizio, fine e tipo della numerazione;

esistono comunque sequenze piu' complesse dette "treni di segnalazione".

E' evidente che il generatore DTMF del modem non prevede anche questi segnali.

Bisogna aggiungere che neppure i 12 toni corrispondenti alle cifre 0-9 # e * sono

esattamente uguali nel DTMF e nel dialogo tra centrali, tuttavia di solito vengono

riconosciute entrambe le serie di frequenze.

Ma e nessun protocollo telefonico internazionale e' un segreto. Basta infilarsi in una libreria universitaria.

A proposito delle intrusioni :

Quando si compone un numero, la centrale locale contatta una centrale remota e

le trasmette alcune informazioni. Tra queste,il numero dell'utente da chiamare,

il tipo di chiamata (utente, operatore, dati, speciale) e la localita' di destinazione (nazione ed area, con un segnale particolare se la chiamata e' interna allo Stato).

Queste info vengono trasmesse con toni concettualmente identici ai DTMF (ma di

frequenza diversa). Inoltre, sempre con toni, le centrali dialogano per stabilire inizio e fine della chiamata ed inizio e fine della sequenza di dial in arrivo da locale a remota.

In particolare una sequenza di questi toni ha un effetto speciale sulla centrale

remota: ordina di eseguire il collegamento con la linea specificata anche se essa risulta gia' impegnata, cioe' l'utente sia gia' al telefono con un'altra persona.

Questa sequenza e' chiamata 'treno di intrusione (o di inclusione)'. Quando una linea subisce una intrusione, il software avvisa l'utente facendogli ascoltare dei toni. Sono quelli che si sentono quando si subisce un 197, prima della orrida voce registrata. Per analogia, anche questi toni vengono chiamati 'intrusione'... cosi' tanto per cambiare abbiamo due cose diverse con lo stesso nome. Tipico della telefonia italiana.

Possono usufruire dell'opzione di intrusione gli operatori (servizi automatici ed 'umani') ma non gli utenti normali ovviamente... infatti se l'ordine di dial che arriva da locale a remota non e' contrassegnato con il codice 'chiamata operatore', l'opzione non e' convalidata e non va in porto.

Non e' la sola caratteristica che differenzia la chiamata operatore da quella utente:

per esempio gli operatori possono chiamare numeri non accessibili all'utente normale.

Premesso che tutte le chiamate telefoniche su tutte le reti (fisse e radiomobili) possono essere intercettate solo sotto richiesta dell'autorità giudiziaria, ed in particolare l'intercettazione risulta abbastanza semplice con la coopearzione dell'operatore telefonico, in questo articolo vengono analizzate le possibilità di intercettare chiamate sulle reti GSM, senza alcuna collaborazione da parte del network telefonico.

Intercettare le conversazioni sui vecchi cellulari analogici TACS è semplice come ascoltare una trasmissione radiofonica; infatti, considerato che le conversazione vengono trasmesse in chiaro, basta possedere uno scanner (il cui prezzo parte da circa 400.000 lire) per essere in grado di ascoltare tutte le chiamate originate o terminate in una determinata cella radio.

Particolari programmi, presenti su Internet, abbinati ad un ricevitore radio controllabile da pc oppure ad un telefono TACS oppurtunamente modificato, consentono anche di filtrare le chiamate sulla base del numero telefonico e di seguirle in caso di cambio di cella radio (handover).

Sulla possibilità di intercettare i telefoni GSM senza l'aiuto dell'operatore, ci sono parecchie discussioni: c'è chi dice che sia possibile, chi invece sostiene che lo standard è assolutamente robusto e la sua sicurezza non può essere compromessa.

La rete GSM, a differenza di quella TACS, è digitale: il segnale prima di essere trasmesso viene convertito in una stringa di numeri. Ciò significa che se si tentasse di intercettare le comunicazioni con un comune scanner, si potrebbe ascoltare solo un ronzio (la trasmissione dei bit).

In ogni canale radio vengono multiplexate contemporaneamente le conversazioni di 8 utenti e ogni conversazione utilizza in sequenza tutti i canali disponibili nella cella radio (Frequency Hopping): in pratica, la durata di utilizzo di una canale radio in modo continuato è pari a 45 microsecondi.

Inoltre la sequenza di bits sulla tratta radio non viene trasmessa in chiaro, ma viene crittografata attraverso l'utilizzo di chiavi (diverse per ogni abbonato).

Pur disponendo delle apparecchiature hardware/software (si potrebbe usare un telefono GSM modificato) in grado di decodificare il segnale digitale, per poter intercettare una conversazione si rendono necessari alcuni parametri, memorizzati sia sulla carta (IMSI=International Mobile Subscriber Identification) che all'interno del network (chiave di autenticazione, chiave di crittografazione).

Tra questi, la chiave di autenticazione viene variata spesso su richiesta del network (in base al settaggio effettuato dall'operatore radiomobile GSM, potrebbe essere variata anche ogni volta che il telefono colloquia con il sistema, ad esempio per comunicare la posizione o per completare una chiamata).

In pratica, riuscire ad intercettare la conversazione risulta estremamente complesso nella tratta radio tra telefono GSM e stazione radio base, ma altrettanto non si può dire per il percorso tra stazione radio base e centrale di commutazione. In questo caso infatti nella maggiorparte dei casi i segnali sono trasmessi in chiaro tanto per i link effettuati con linee terrestri quanto per quelli realizzati con sistemi a microonde.

La vulnerabilità della tratta tra stazione radio base e centrale di commutazione è stata dimostrata lo scorso anno dal Dottor Ross Anderson dell'Università di Cambridge, in occasione di un concorso indetto dalla compagnia tedesca Mobilcom. Il ricercatore, che ha vinto il premio in palio di 100.000 marchi tedeschi, è riuscito ad inserirsi nella rete GSM, facendo una chiamata a carico di un altro numero.

Attualmente esiste un sistema che è in grado di intercettare tutte le conversazioni di uno specifico abbonato GSM, senza la collaborazione dell'operatore radiomobile.

Tale sistema, progettato dalla Gcom Technology, è stato realizzato modificando una stazione radio base GSM e compattandola in un box di piccole dimensioni.

Come funziona.

E' necessario attivare il box Gcom in prossimità dell'abbonato che si vuole intercettare.

La nuova stazione radio base si presenta al telefonino target (ma anche a tutti quelli del circondiario) come se fosse parte integrante della rete GSM reale.

Dal momento che la stazione Gcom genera un canale di controllo con un segnale più forte rispetto a quello della rete GSM reale, il telefonino, dopo aver effettuato delle misure di segnale, si registra sulla stazione fittizia.

La stazione Gcom si presenta al network GSM reale, come un telefonino GSM, che contiene i dati dall'abbonato target.

Da questo momento in poi tutte le chiamate da e verso il telefonino verranno completate attraverso la stazione radio base Gcom, collegata in modo trasparente alla rete GSM. Le conversazioni intercettate sul telefonino target possono quindi essere registrate in locale e/o essere inviate automaticamente attraverso una linea GSM ad un centro di controllo.

Naturalmente questo sistema è molto complesso da utilizzare (richiede una competenza specifica elevata) ed inoltre, dal punto di vista economico, non è alla portata di tutti.

Inoltre per un corretto funzionamento è necessario conoscere con esattezza la posizione dell'abbonato e se questo è in movimento è necessario seguirlo.

Naturalmente le capacità di intercettazione che ha l'operatore sono nettamente superiori a quelle offerte dal sistema Gcom.

Ricordiamo che l'operatore, oltre alla possibilità di intercettare le chiamate, è anche in grado di conoscere la posizione di ogni abbonato con una buona approssimazione. Infatti il sistema conosce in ogni momento il tempo impiegato dal segnale radio per andare dalla stazione radio base al telefono GSM e viceversa.

Una migliore approssimazione (qualche decina di metri) è possibile attraverso la triangolazione se il telefono si trova sotto il raggio di copertura di più celle; infatti il segnale del telefono è ricevuto anche dalle celle radio adiacenti a quella in cui il telefono è loggato, che conoscono con esattezza il ritardo di propagazione del segnale (da questo si risale alla distanza).

Mercoledì 5 Giugno 2002

Security e VeriSign hanno annunciato un nuovo servizio che dovrebbe consentire agli operatori di intercettare più facilmente le telefonate. Il sistema, denominato NetDiscovery, è ancora nella fase di test e sarà disponibile commercialmente a luglio di quest'anno. E' adatto alle linee fisse, alle reti mobili e ai sistemi su cavo. In base alle norme dettate dal Communications Assistance for Law Enforcement Act del 1994, gli operatori devono avere sistemi che consentano alle autorità investigative di intercettare rapidamente le telefonate delle persone sottoposte ad indagine su mandato dell'autorità giudiziaria. Le norme prevedono che gli operatori forniscano all'FBI o alla polizia locale i risultati delle intercettazioni. Inizialmente gli operatori avevano tempo fino al 30 settembre 2001 per mettersi in regola con queste norme. In seguito la data è stata spostata al 30 giugno 2002, a causa dei notevoli costi che l'adeguamento comporta per gli operatori. Con il lancio del nuovo servizio, gli operatori hanno la possibilità di affidare tale adeguamento in outsourcing a VeriSign in cambio di un canone mensile, il che eviterebbe le grandi spese per l'aggiornamento dei sistemi.

GSM: a causa delle modulazione digitale non e' possibile l'ascolto delle conversazione attraverso un normale scanner. L'unico possibilità e la ricezione dei burst (pacchetti di dati trasmessi sul canale radiofonico) e la loro successiva analisi e decodifica. Vari gruppi di lavoro stanno studiando l'algoritmo A5 (versione AX) che viene utilizzato per la criptazione dei dati trasmessi via radio