LA TEORIA DELLE COMUNICAZIONI SU RETE GSM

Le specifiche tecniche delle reti GSM sono state implementate nell'anno 1994 dal GSM Consortium in considerazione di due priorità:
1) Un sistema standard a livello mondiale.
2) Un sistema particolarmente sicuro, soprattutto per difendersi dalla clonazione degli apparati (tecnica illegale molto diffusa con i vecchi terminali analogici ETACS, detti anche di "prima generazione").

Un network GSM si compone essenzialmente di 4 sottosistemi:
1) MOBILE STATION (MS o terminale): una sorta di ricetrasmettitore particolarmente evoluto, il "telefonino".
2) BASE STATION SUBSYSTEM (BSS o "ponte"): è composta a sua volta di due elementi strutturali: la BTS (Base Transceiver Station) che si occupa di stabilire un contatto radio full duplex con il terminale GSM, e la BSC (Base Station Controller) che interagisce con la rete cellulare e con le altre BTS in zona.
3) NETWORK SUBSYSTEM (NS o nodo di commutazione): funziona come nodo di commutazione per una determinata zona, provvedendo altresì all'impostazione delle chiamate e alle procedure di autenticazione.
4) OPERATION AND SUPPORT SUBSYSTEM (OSS o "centrale"): è il "cervello" elettronico che gestisce in maniera centralizzata e computerizzata tutto il network GSM di un determinato operatore di telefonia mobile, vero cuore motore e punto nevralgico del sistema, l'unico punto dove l'intercettazione di una comunicazione GSM può avvenire all'occorrenza in maniera semplicissima e quasi immediata.

Esistono vari ostacoli per poter intercettare e decodificare un segnale GSM fuori dalla OSS: innanzitutto i segnali radio non sono "in chiaro", cioè non sono comprensibili all'orecchio umano, ma si presentano criptati con chiavi diverse per ogni utente e vengono trasmessi compattati in pacchetti digitali (burst); L'orecchio umano, sintonizzando con un comune ricevitore radio i segnali trasmessi dai GSM, può percepire solo una sorta di "ronzio" privo di ogni comprensibilità. Con questa tecnica di trasmissione un singolo canale radio può ospitare contemporaneamente numerose conversazioni.

Gli algoritmi di codifica utilizzati dal sistema GSM sono essenzialmente 3:
1) L'algoritmo A3 (protegge il codice di identificazione dell'abbonato ed è memorizzato nella SIM card);
2) L'algoritmo A8 (algoritmo a 128 bit che protegge la "chiave personale di autenticazione" o "chiave di partenza" ed è memorizzato nella SIM card. La chiave personale di autenticazione è utilizzata anche per la generazione delle chiavi temporanee a 64 bit dette "chiavi di sessione"); Sebbene a 128 bit, l'algoritmo A8 è considerato tutt'altro che sicuro, vedremo oltre il perchè.
3) L'algoritmo "stream cipher" A5/Ax (algoritmo a 64 bit custodito nell'hardware del terminale e nella BTS o "ponte"); anche questo algoritmo sembra essere piuttosto vulnerabile, a dispetto dei suoi 64 bit, indebolito forse volutamente. E' questo terzo algoritmo il diretto criptatore delle conversazioni trasmesse via radio.
Un ruolo fondamentale è rappresentato dalla SIM card, un microchip della famiglia delle "smart-card" che contiene due algoritmi di codifica, tre codici utente oltre a numerosi altri dati memorizzati in maniera sia volatile che non volatile.
Tali algoritmi interagiscono fra di loro sulla base di una chiave di partenza fissa protetta dall'algoritmo A8 a 128 bit (chiave personale di autenticazione memorizzata nella SIM card) e generano costantemente altri elementi variabili ad ogni chiamata e ad ogni accesso alla rete, per talune funzioni anche in maniera ciclica. Queste iterazioni sono strutturate in maniera tale le credenziali di identificazione non vengano mai trasmesse sul canale radio (tecnica di "challenge response"), fatta eccezione per il codice identificativo criptato dell'utente (IMSI) ma solo limitatamente ad un istante (vedi sotto); La chiave "di partenza", che fa capo all'algoritmo a 128 bit, interagisce ad ogni connessione con il network al fine di consentire da parte dello stesso la generazione casuale della seconda chiave (questa volta temporanea, cioè variabile ad ogni chiamata) detta "chiave di sessione" (codice random a 64 bit). La "chiave di sessione" generata dal network giunge dal network fino alla BTS (ponte) ma non viene mai trasmessa via radio.
Quindi per poter intercettare una conversazione di uno specifico utente si renderebbero necessari di volta in volta un intero pacchetto di parametri, (fissi e variabili) presenti sia sulla SIM card sia nel network dell'operatore. Ribadiamo, ad ulteriore conferma della sicurezza e complessità del sistema, che alcune chiavi di questi algoritmi di criptazione sono variabili. Il sistema GSM protegge anche l'invio in rete dell'IMSI (International Mobile Subscriber Identification, un codice fisso in grado di identificare in maniera univoca un utente), sostituendolo temporaneamente ad ogni chiamata con un codice random detto "TMSI" (Temporary

Mobile Subscriber Identification o codice di identificazione provvisoria). Il codice TMSI viene scritto in una partizione volatile della SIM e varia ad ogni accesso alla rete. In questo modo il sistema GSM maschera anche l'unico codice fisso che per un breve istante (e inevitabilmente!) deve essere trasmesso via radio, cioè l'IMSI.
In sintesi il sistema GSM è tutt'altro che semplice da attaccare, ORIGINARIAMENTE FORSE TROPPO SICURO PER "QUALCUNO" CHE NON HA GRADITO QUESTA BLINDATURA (vedi oltre).

I CODICI DI CRIPTAZIONE

L'argomento "intercettazione GSM" e' molto dibattuto, e più volte si sono succeduti annunci relativi all'avvenuta scoperta di un sistema pratico e utile per ottenere la chiave di decodifica dell'algoritmo "stream cipher" A5/Ax, considerato la base di partenza per ottenere (assieme alla disponibilità dei parametri memorizzati nella SIM card, prima fra tutti la chiave personale di autenticazione) l'intercettazione di una comunicazione GSM "real time" relativa ad un utente specifico; poi, puntualmente, la smentita. Secondo uno dei massimi esperti di criptazione digitale, l'inglese Anderson, alcuni ricercatori sarebbero prossimi ad ottenere un sistema relativamente rapido per decodificare "brute force" i pacchetti burst nelle tratte terminali dei network GSM (comunicazione fra ponte radio terrestre, o "BTS", e terminale GSM). Tali proclami però sono essenzialmente teorici ed accademici.
Il "segreto" relativo all'algoritmo A5/Ax sarebbe relativamente "semplice", a dispetto della complessità d'insieme dell'argomento: si e' sempre ritenuto che il codice A5/Ax fosse basato su una chiave composta da 64 bit, mentre ora sembra ormai certo che gli ultimi 10 bit di dati sono sempre volutamente resi pari a "0". La differenza, apparentemente insignificante, comporta invece un vantaggio tangibile per gli addetti ai lavori: una chiave a 64 bit, completamente sconosciuta, richiede ANNI di elaborazione di un computer molto potente (non parliamo certo di PC domestici!) per essere ricercata. Sono infatti una cifra stellare le combinazioni matematiche possibili. Invece un codice indebolito artificialmente da una sequenza fissa e nota, a parità di potenza di elaborazione, "solo" poche ore. Questo però è un vantaggio essenzialmente rivolto alle intelligence dei paesi più evoluti. Servono tempi molto più ridotti ma soprattutto metodi molto più semplici per operare efficaci intercettazioni "real time" con potenze di calcolo standard, quindi su questo specifico fronte siamo comunque lontanissimi dal sistema accessibile a chiunque.
L'altro codice di criptazione A8 che protegge la chiave personale di autenticazione residente nella SIM, è stato dimostrato essere altrettanto attaccabile, a dispetto dei 128 bit che sembrano essere garanzia di massima sicurezza. Basta disporre fisicamente della SIM card, di un lettore "smart card" e un PC equipaggiato con un programma apposito. I tempi per ottenere questo fondamentale codice fino all'anno scorso superavano le 20 ore di elaborazione con un comune PC equipaggiato con processore Pentium 600, ma la IBM ha annunciato nel 2003 di aver messo a punto un software in grado di compiere questa operazione in pochi secondi; Il motivo alla base di questo risultato tutt'altro che stupefacente: anche questo algoritmo è stato indebolito in maniera controllata e voluta! Ricordiamo che una chiave di criptazione a 128 bit di tipo "forte" (quindi di elevata qualità), richiederebbe teoricamente centinaia di anni di elaborazione da parte del computer più potente attualmente disponibile per essere trovata. Per un computer domestico parliamo di molte migliaia di anni.
A conferma definitiva che quanto contenuto nella SIM CARD non è certo inviolabile, è giunta sempre nel 2003 la notizia di un software in grado di emulare completamente il funzionamento di una SIM; con questo software (oltre ovviamente ad un terminale GSM connesso al PC), è possibile fare e ricevere telefonate senza SIM CARD fisiche connesse al telefono; al momento questo sistema non sembra in grado di intercettare comunicazioni altrui, ma potrebbe anche trattarsi del punto di svolta atteso per imprimere una decisa accelerazione alle ricerche.
Da segnalare infine l'enigmatica notizia giunta da Israele a fine 99: si tratta di un annuncio riguardo alla possibilità di intercettare i GSM in maniera realmente semplice ed economica. Secondo due ricercatori dell'università di Tel Aviv (Alex Biryukov e Adi Shamir) sarebbe addirittura sufficiente uno scanner radio qualsiasi, interfacciato ad un computer Pentium e un capiente disco rigido. L'apparente eccessiva semplicità ha fatto supporre addirittura la scoperta di un "bug" macroscopico nei network GSM. Poi non si è saputo più nulla e la notizia si è persa nel silenzio totale. Cosa c'era di fondato? E' lecito supporre che "qualcuno" sia intervenuto per zittire due ricercatori un po' troppo.... zelanti? Questo sistema, se realmente esiste, potrebbe essere utilizzabile ancora oggi o la presunta falla è stata nel frattempo rimediata dai gestori di telefonia mobile?

CHI HA VOLUTO L'INDEBOLIMENTO DEL CODICE A5 E PERCHE'?

Esistono varie versioni dell'algoritmo base A5 (vedi sopra), il codice che protegge i segnali digitali trasmessi via radio. Il sistema paneuropeo è uniformato su una sottoversione (Ax), concepita fin dall'inizio per non offrire un livello di sicurezza assolutamente inattaccabile. Il primo giallo sul codice algoritmico A5 risale nientemeno che al giugno 1994, quando il professor Simon Sherpherd della Bradford University di Londra

decise di tenere un convegno per denunciare (presumibilmente) di avere scoperto qualcosa di strano nell'architettura del codice A5 ed in particolare della sua versione AX, di fatto sembra la scarsa qualità dell'algoritmo. E' provato che il GCHQ (servizio segreto di intelligence inglese) intervenne repentinamente e il convegno fu annullato "per indisposizione" del professore, in perfetto stile KGB. Ovviamente il professore non era mai stato meglio di così! Il convegno non fu mai più riorganizzato, nonostante le pressioni degli esperti e degli interessati al tema. Siamo nel 1998 quando David Wagner e Ian Goldberg, ricercatori dell'Università di Berkley - California e legati all'Internet Security Applications Authentification and Cryptography Group (ISAAC), sollevarono sensazione comunicando di avere scoperto anche loro la conferma matematica di un indebolimento (definito "evidentemente pilotato") del codice A5. Ma David Wagner e Ian Goldberg, dopo aver "infranto" l'algoritmo A5, andarono decisamente oltre e attaccarono con pieno successo gli altri due algoritmi rimasti: A3 e A8, entrambi residenti nella SIM CARD, demolendoli inesorabilmente. Si aprì quindi una strada molto interessante, cioè la decodifica dei dati contenuti nel Subscriber Identification Module (SIM), l'ultimo ostacolo rimasto.
Per una ulteriore conferma ci ha messo lo zampino anche l'Italia, per tramite dei professori della facoltà di Ingegneria Informatica di Padova Marcello Scatà e Lorenzo Romano: secondo loro (convinti che il codice sia in realtà di soli 40 bit di dati e per di più indebolito da concatenamenti non casuali) i tempi per decodificarlo sarebbero di soli 12,7 giorni con un comune personal computer (poche ore con i potenti elaboratori a disposizione degli enti governativi). Secondo gli esperti dell'Università di Berkley invece, come già abbiamo detto, il principale elemento che indebolisce volutamente l'algoritmo sarebbe da ricercare negli ultimi 10 bit di dati, sempre fissi a zero. La sostanza non cambierebbe in maniera molto significativa, se è vero che altre parti dell'algoritmo rispondono a sequenze logiche e prevedibili nel contesto di un calcolo strutturato, quindi tutt'altro che casuali come dovrebbero.

Per parafrasare la nota Agatha Christie, un indizio è sempre un caso, due indizi possono ancora essere un caso, sebbene molto strano, ma tre indizi rappresentano sempre una ragionevole certezza....

Le sottoversioni paneuropee del codice A5 sembrerebbero sicure fino al punto da essere inattaccabili da parte di soggetti dotati di computer domestici e conoscenze non evolute, ma l'indebolimento consentirebbe invece la decodifica on-the-air a patto di disporre di strumenti molto più specifici. Una delle tecniche adottate sembra essere piuttosto semplice: vengono registrati i pacchetti burst trasmessi su tutti i canali radio GSM impegnati in una determinata zona, dopodichè la "conversazione digitale" viene decodificata nel giro di qualche ora. Quindi qualcuno ha voluto che la sicurezza dell'algoritmo A5 venisse ridotta in maniera contenuta, e tale algoritmo costituirebbe un valido ostacolo ormai solo per i livelli medi e bassi dei vari organismi di intelligence.

INTERCETTARE I GSM IN PRATICA

Allora quali sono le tecniche per intercettare le conversazioni che avvengono tramite un cellulare GSM, escludendo investimenti in potentissimi computers e in tecnologie ad alto livello?

1) **MONITOR:** in assoluto i più diffusi. Sono sistemi portatili che, di fatto, svolgono funzioni del tutto simili ad un ponte radio GSM. Questi apparecchi, introdotti per la prima volta da GCOM Technologies e poi copiati da altri laboratori, si sostituiscono in maniera forzata al ponte ufficiale del gestore, consentendo di decodificare il segnale radio come del resto fa qualsiasi ponte (ovviamente dopo che è avvenuto l'interfacciamento con la centrale del gestore tramite un ponte radio BTS reale altrimenti, come già detto, ogni forma di decriptazione "stand alone" senza i dati della SIM CARD è a tutt'oggi considerata solo alla portata di pochissimi). In pratica il sistema, dopo avere acquisito i dati dell'utente come farebbe una qualsiasi BTS, si presenta al ponte radio più vicino come il cellulare GSM che stà effettuando la chiamata, e al cellulare GSM come il ponte radio terrestre (BTS). Ma non mancano i limiti e le controindicazioni. Innanzitutto bisogna essere molto vicini al cellulare sotto controllo (100-200 mt. al massimo), poi il sistema è critico da mettere a punto, ingombrante e con costi stratosferici. Infine (ma certamente è un aspetto non trascurabile in certi casi!) la compatibilità non è universale, bensì condizionata da alcuni parametri chiave legati all'operatore di telefonia mobile. E' quindi un complesso sistema "filtro" per monitorare il traffico a breve distanza.
2) **SIM CARD CLONATA:** Negli ultimi mesi del 2001 ha preso consistenza questa tecnica. Bisogna disporre fisicamente per qualche tempo della SIM CARD del telefono da intercettare per poter procedere alla clonazione. Dopodichè è sufficiente un personal computer, un qualsiasi terminale GSM e un particolare software basato in pratica sulle scoperte effettuate nel 1998 dai ricercatori dell'Università di Berkley (CA - USA, vedi sopra). Il sistema, nella sua prima versione, registrava la conversazione off-air e la decodificava, rendendola perfettamente ascoltabile. Sistemi basati sulla clonazione della SIM CARD, sono stati presentati nel Dicembre 2001 durante un convegno di Hackers tenutosi a Berlino ed organizzato dal famoso CCC (Chaos Computer Club): troppa

pubblicità però..... inganna! gli operatori di telefonia mobile sono corsi ai ripari introducendo nel network GSM un sistema per bloccare questa possibilità.

3) **CIMICI:** tecnica in realtà indiretta. Viene fatto ricorso alle cimici, collocate nei luoghi ove ragionevolmente si ritiene che il soggetto sorvegliato effettuerà la sua conversazione (casa - auto, ecc.). Non vi sono certezze, ma ragionevoli possibilità di intercettazione. Il relativo basso costo di queste "antiche" tecnologie rende possibile l'utilizzo di numerosi pezzi opportunamente dislocati in maniera tale da coprire logisticamente i luoghi dove il sorvegliato potrebbe presumibilmente utilizzare il GSM. Ovviamente l'ascolto è "simplex" cioè si ascolta solo uno dei due interlocutori. Questo però è spesso più che sufficiente a definire e inquadrare l'oggetto della conversazione.
4) **BATTERIE DEI CELLULARI**: la crescente miniaturizzazione degli apparecchi e l'irradiazione di radiofrequenza del GSM rende complessa questa pratica. L'operazione è ancora praticabile in un numero molto ridotto di casi e con i limiti di portata rappresentati dalla potenza del modulo microtrasmittente, che deve essere alimentato dalla stessa batteria che alimenta in cellulare (parliamo di circa 100 metri utili).
5) **TRATTA TERRESTRE:** se riuscire ad intercettare la conversazione GSM risulta estremamente complesso nella tratta radio tra terminale GSM e BTS, altrettanto non si può dire per il percorso tra stazione radio base e centrale dell'operatore. In questo caso i segnali sono trasmessi in chiaro o con sistemi di protezione tutt'altro che inattaccabili. Appena lasciata la BTS infatti il traffico viaggia su cavo. Una derivazione dal cavo telefonico in uscita dalla BTS potrebbe essere praticabile e relativamente semplice.
6) **ALTRI SISTEMI** (vedi oltre).

COME GLI ORGANI INVESTIGATIVI UFFICIALI INTERCETTANO I GSM?

Le conversazioni tramite GSM "sotto controllo", come ampiamente dimostrato dalle cronache quotidiane, vengono intercettate e registrate dagli organi inquirenti ufficiali previo decreto della Magistratura. I tempi per ottenere l'autorizzazione variano da poche ore ad alcuni giorni, secondo l'urgenza delle indagini, e in questo modo le intercettazioni possono avvenire con la collaborazione tecnica dell'operatore di telefonia mobile, quindi nella maniera più semplice, rapida ma soprattutto affidabile. La centrale dell'operatore di telefonia mobile è l'unico punto dove transita in maniera centralizzata tutto il traffico di rete (livello OSS). E' l'operatore di telefonia mobile che può chiudere e aprire rapidamente determinati "interruttori" per far ascoltare e/o registrare il traffico senza vincoli legati alla distanza dal GSM da controllare e senza dover intervenire in qualche modo su SIM CARD o telefonino.

TECNOLOGIE CUSTOM PER L'INTERCETTAZIONE GSM

Piccola rassegna di tecnologie ormai da tempo ufficializzate, in grado di intercettare una trasmissione GSM senza alcuna collaborazione tecnica da parte dell'operatore di telefonia mobile, senza dover preventivamente entrare in possesso della SIM card del numero da intercettare e senza sostituire o modificare alcunchè nel telefonino controllato. Stiamo parlando in primis dei ponti GSM fittizi con varianti e sottovarianti tecniche. La trattazione che segue è limitata alle tecnologie che chiunque può reperire su Internet a seguito di una semplice ricerca, quindi le cui informazioni sono reperibili e dsponibili liberamente. Noi ci siamo limitati a raccoglierle e catalogarle al solo fine di rispondere ad alcune domande frequenti in tema di intercettazione dei GSM, che troppo spesso vedono alla base disinformazione e leggende metropolitane. Va da se che chiunque volesse realmente acquistare questi "aggeggi" lo deve fare direttamente e a suo rischio e pericolo, sia dal punto di vista delle garanzie di reale funzionamento (per quanto ne sappiamo dubbie) sia per implicazioni legali connesse alle eventuali pratiche di intercettazione. Electronet ha solamente raccolto quanto già da tempo pubblicamente reperibile e disponibile agli occhi di chiunque "sfogli" la rete delle reti.

Il GSM2065 della californiana DPL. Per pochi spiccioli (circa 450000,00 euro... si, avete letto bene, quattrocentocinquantamila euro) è possibile assicurarsi il sistemino per ascoltare i GSM. Non abusatene per favore, magari prestandolo all'amico in vena di scherzi! "Si dice" che dovrebbe intercettare a circa 100mt. dal cellulare da controllare, se va bene anche qualcosa di più, molto dipende dalla distanza della BTS reale e dagli ostacoli ambientali nei dintorni. Per procedere all'acquisto fare un salto in California. Dovrebbe essere una questione rapida, in perfetto stile USA, basta che il sistema venga pagato cash e portato subito fuori dagli USA. Roba per pochissimi.

Per fortuna che ci sono i GSM interceptor IN OFFERTA SPECIALE! E' una proposta molto simile a quella sopra, ma questa viene appena 350000 euro, quotazione online ufficiale "aperta al pubblico"; se vi accontentate di intercettare solo negli USA (standard 1900MHz) sono sufficienti 230000 euro (speriamo che nei 230000 euro sia compresa quella bella antennina visibile a destra, quella davvero ci piace da matti!). Intercetta a un centinaio di mt. dal cellulare da controllare. Qualcosa del genere circola in alcune pagine web italiane, come i più attenti probabilmente avranno notato. Per averlo veramente dovrebbe essere sufficiente contattare la statunitense Accelerated-promotions tenendo presente che solo la demo del sistema viene circa 8300,00 euro anticipati, prendere o lasciare. Garantito e assistito (ci mancherebbe!). Al costo di cui sopra consigliamo di aggiungere il biglietto aereo per andarselo a prendere; con quello che costa l'interceptor si può viaggiare comodamente in Business Class e fare anche una capatina a Las Vegas: i relativi costi saranno una goccia nel mare rispetto ai verdoni necessari per acquistare l'interceptor delle meraviglie.

Carino, in tutti i sensi! Anche questo deja vu su alcune pagine web.... italiche. Dealers ufficiali? Mah, serissimi dubbi! Per evitare problemi di copyright (noi di solito ci stiamo attenti, a differenza di altri) precisiamo che la foto l'abbiamo reperita sul sito ufficiale del produttore, che qui citiamo in quanto liberamente reperibile da chiunque con facilità. A chi interessa vendere l'attico in città e il bilocale al mare per comprarsi questo gioellino lasciamo gli estremi così come noi li abbiamo trovati: **http://www.securtelecom.com** Tornando seri il GSM Monitoring System della ditta indiana Secur Telecom sfiora i 400000 euro (!)
Dimenticavamo di dire che il sistema viene garantito "semplice da usare" (certo, basta guardarlo per capire che è facile come usare un tostapane!).
Il produttore scrive "solo per enti governativi", ma siamo ragionevolmente ottimisti sul fatto che se andassimo in India con le tasche traboccanti di dollaroni e un bel sigaro in bocca ce lo porteremmo a casa anche se non siamo la CIA. Forse accettano anche euro, pardon, **euri** (consentiteci la licenza, visto che sono davvero tanti!) Garantito e assistito, la sola demo costa quanto una Fiat Punto nuova fiammante. Roba da ricchi, molto ricchi.

La ditta Scadecas http://scandecas.com ci propone il JBR01 regolarmente online da tempo e pubblicizzato senza restrizioni di sorta; anche questo costa talmente tanto che non se lo potrebbe permettere manco Totti (almeno fino a quando Berlusconi non ci ridurrà le tasse, ricordate?) ma da rumors sembra che ci siano repliche piratate reperibili in qualche paesino nelle steppe russe. Se volete rinnovare la "Campagna di Russia" armiamoci e parti**TE**, noi restiamo al calduccio del nostro ufficietto italico e non investiamo manco un euro per andare a prendere una fregatura. Deve essere stato questo che intendeva Putin quando qualche mese fa ha tuonato alla Duma: "Bisogna ridurre il gap tecnologico con l'occidente sui sistemi spionistici!" detto... fatto!

ALTRO: vi sarebbero altre tecniche, strategie & stratagemmi, alcune improbabili, altre relativamente efficaci, anche con costi contenuti ma con tangibili limitazioni tecniche e pratiche; sopra a tutti i clone degli oggetti di

cui sopra, che consentono di poter togliere uno zero dalle cifre esposte ma senza assistenze e garanzie, in pratica un “visto e piaciuto” che gela un po’ il sangue in quanto (forse) il sistema funziona oggi, ma domani? Poi appaiono periodicamente su Internet una serie di trucchi tecnologici per aggirare l’ostacolo della decriptazione sfruttando falle e “sviste” di vario tipo, spesso imputabili ai contratti e/o alle procedure dell’operatore di telefonia mobile (rif. vari siti di GSM hacking et similia). Talvolta tali sistemi sono estremamente macchinosi; in altri casi, al contrario, incredibilmente semplici. Anche questi avrebbero una caratteristica pittoresca, cioè con una buona dose di fattore “C” possono funzionare oggi, domani forse, dopodomani chissà, possono funzionare con un operatore, ma forse non con l’altro, possono funzionare forse in Francia, ma probabilmente non in Germania, ecc. Di certo sono tutti e sempre a funzionamento garantito e certo laddove non c’è copertura GSM ☺ Fra le soluzioni per aggirare l’ostacolo delle criptazioni sembra che esistano anche telefonini con doppio circuito GSM (chiamerebbero un altro numero se il GSM controllato viene usato) e telefonini con il microchip registrante che si attiva solo quando il GSM è in trasmissione. Immaginiamo che siano gioielli di miniaturizzazione, sempre che esistano veramente, ma del tutto inutili se non si può “regalare” un determinato e preciso apparecchio alla persona che si vuole controllare.

Da 10 anni una folta schiera di tecnici, studiosi ed esperti di tutto il mondo hanno fatto dell’attacco alla sicurezza dei GSM una sorta di questione di principio..... qualcosa devono pure aver partorito tutte queste menti più o meno orientate verso un’unico scopo!

****

PER APPROFONDIRE

IL NUOVO ALGORITMO A5/3 KASUMI

Luglio 2002: la francese Europe's Telecommunications Standards Institute (ETSI) ha annunciato l'avvenuta creazione di un nuovo algoritmo, fra i più sofisticati mai adottati nelle comunicazioni wireless. L'algoritmo è stato battezzato A5/3. A5/3 codifica i messaggi di segnalazione degli operatori di telefonia mobile, in modo tale da proteggere efficacemente anche informazioni come numeri di telefono e i dati utente.
Sebbene sia stato sviluppato specificamente per le reti 2G/2,5G, l'A5/3 si basa su Kasumi, un algoritmo messo a punto recentemente e che verrà utilizzato nelle reti UMTS. Kasumi è considerato assolutamente inattaccabile, come del resto era stato detto anche per i vecchi algoritmi attualmente in uso nelle reti GSM; sappiamo poi che le cose sono andate diversamente, anche se non si può negare che dopo molti anni di servizio le reti GSM offrono ancora un elevato standard di sicurezza. L'ETSI ha spiegato che il nuovo algoritmo è utilizzabile anche sulle reti GPRS, EDGE e HSCSD, ed è stato progettato per durare almeno 15 anni. Rispetto al suo predecessore, nato 14 anni fa, l'A5/3 proteggerà con efficacia il crescente volume di traffico dati wireless, oltre ovviamente alle comunicazioni vocali. Inutile sottolineare che, visti i tempi che corrono, appare assai improbabile che ai maggiori organi investigativi mondiali venga preclusa la possibilità di intercettare i GSM senza la collaborazione dell'operatore di telefonia mobile. Realistico supporre che una qualche forma di "passepartout" dovrà esistere, e forse è già stato prevista (o meglio..... imposta).

Aggiornamento maggio 2004: A5/3, il nuovo algoritmo di criptazione per reti GSM, resterà nel cassetto. I principali operatori mondiali di telefonia mobile hanno infatti annunciato che l’implementazione del nuovo sistema di sicurezza comporterebbe un impatto economico eccessivo.

Un documento esclusivo: la prima denuncia ufficiale della scoperta di una falla voluta nel sistema GSM

FLAW IN CELL PHONE ENCRYPTION IDENTIFIED; DESIGN PROCESS BLAMED
Telecommunications Industry Association algorithm for digital telephones fails under simple cryptanalysis

MINNEAPOLIS, MN. AND BERKELEY, CA., March 20, 1997 - Counterpane Systems and UC Berkeley jointly announced today that researchers have discovered a flaw in the privacy protection used in today's most advanced digital cellular phones. This discovery points to serious problems in the closed-door process used to develop these privacy measuers. This announcement is a setback to the US cellular telephone industry, said Bruce Schneier of Counterpane Systems, a Minneapolis, MN consulting firm specializing in cryptography. The attack can be carried out in a few minutes on a conventional personal computer.

Schneier and John Kelsey of Counterpane Systems, along with graduate student David Wagner of the University of California at Berkeley, plan to publish their analysis in a paper entitled "Cryptanalysis of the Cellular Message Encryption Algorithm (CMEA)." Legislators are scheduled to hold hearings today on Rep. Goodlatte's "SAFE" (Security And Freedom Through Encryption) bill, HR695.

The problem affects numbers dialed on the key pad of a cellular handset, including any telephone, PIN, or credit cards numbers dialed.

The system was supposed to protect the privacy of those dialed digits, but the encryption is weak enough that those digits are accessible to eavesdroppers with a digital scanner.

The cryptographers blame the closed-door design process and excessive pressure from U.S. military interests for problems with the privacy standard. The cellular industry attempted to balance national security with consumer privacy concerns. In an attempt to eliminate recurring security problems, the cellular standards arm of the Telecommunications Industry Association (TIA) privately designed this new framework for protecting cellular phones. The system uses encryption to prevent fraud, scramble voice communications, and protect users' privacy. These new protections are being deployed in today's digital cell phones, including CDMA, NAMPS, and TDMA.

Not a new problem
As early as 1992, others - including noted security expert Whitfield Diffie - pointed out fatal flaws in the new standard's voice privacy feature. The two flaws provide a crucial lesson for policy makers and consumers, the researchers said. These weaknesses are symptomatic of broad underlying problems in the design process, according to Wagner.

Many have criticized the National Security Agency (the U.S. military intelligence agency in charge of electronically monitoring foreign powers) for insinuating itself into the design process, pressuring designers to cripple the security of the cellular encryption technique and hamstringing emerging cellular security technology. "The result is weaker protection for everybody," Kelsey said.

"This is another illustration of how U.S. government efforts to control cryptography threaten the security and privacy of Americans," said David Banisar, attorney for the Electronic Privacy Information Center in Washington, D.C.

This is not the first report of security flaws in cellular telephony. Today, most cellular phone calls can be intercepted by anyone in the area listening to a scanner, as House Speaker Newt Gingrich learned this past January when someone with a scanner recorded one of his cellular calls. According to FCC estimates, the cellular telephony industry lost more that $400 million to fraud and security problems last year.

CMEA Technology
CMEA is a symmetric cipher, like the Digital Encryption Standard (DES). It uses a 64-bit key, but weaknesses in the algorithm reduce the key to an effective length of 24 or 32 bits, significantly shorter than even the weak keys the U.S. government allows for export.

Greg Rose, program chair of the 1996 USENIX Security Symposium, put the results in context: "This break does not weaken the digital cellular fraud protections. And it's still true that digital cellular systems are much harder to casually eavesdrop on than analog phones. But it's clear from this break that a determined criminal with technical resources can intercept these systems."

Counterpane Systems is a Minneapolis, MN-based consulting firm specializing in cryptography and computer security. Bruce Schneier is president of Counterpane and author of three books on cryptography and security. David Wagner is a founding member of the ISAAC computer security research group at UC Berkeley. In the Fall of 1995, the ISAAC group made headlines by revealing a major flaw in Netscape's web browser. The authors also hasten to thank Greg Rose for his advice.

IL PIU' COMPLETO GLOSSARIO DELLA TELEFONIA MOBILE

Alfanumerico
Termine che indica l'insieme dei caratteri numerici e letterali. Il numero di telefono e il nome cui esso è associato costituisce un insieme di dati alfanumerici.

ALM
Advanced Load Management. Tecnica adottata nel sistema Dual Band per permettere la commutazione automatica tra le reti a 900 e 1800 Mhz, in modo da utilizzare in ogni momento il migliore segnale di copertura.

ALS
Alternative Line Service. Tecnica che permette di gestire due numeri di telefono con la stessa SIM Card (non disponibile in Italia, per il momento).

AMPS
Advanced Mobile Phone System. Standard analogico molto usato nell'America settentrionale.

Analogico
Sistema di ricetrasmissione telefonica basato sulla modulazione analogica del segnale radio, la cui forma segue quella della voce. Questo sistema presenta diversi difetti e limitazioni, come la facile clonazione, l'intercettazione delle telefonate, le cadute di linea, un minor numero di canali disponibili, una forte limitazione nei servizi aggiuntivi. Il sistema che risolve buona parte di questi problemi è quello digitale.

AoC
Advise of Charge. Sistema che consente la visualizzazione sul display del credito residuo per le schede prepagate.

Autenticazione
Procedura da eseguire per rendere impossibile la clonazione di un apparecchio analogico E-TACS.

Autoredial
Ricomposizione automatica dell'ultimo numero chiamato.

Bluetooth
Tecnologia di scambio dati via onde radio a 2.4 Ghz, con copertura da 10 a 100 metri anche in presenza di ostacoli. E' stata scelta da Ericsson, Nokia e altri per consentire lo scambio di voce e dati tra apparecchi simili o differenti, come cellulari, palmari, computer, pager, modem. La trasmissione è omnidirezionale e punto-multipunto.

CAI
Common Air Interface. Standard europeo che stabilisce le caratteristiche dello scambio di dati digitali senza fili.

Call Barring
Blocco delle chiamate. Serve per impedire alcuni tipi di chiamata da un apparecchio cellulare (ad esempio, tutte quelle internazionali).

CAP
Cordless ad Accesso Pubblico. Nel sistema DECT identifica i cordless che possono anche collegarsi alla rete Fido di TIM.

Caricabatteria
Ne esistono di vari tipi. I più comuni funzionano con la corrente elettrica e possono essere di tipo rapido (con tempo di ricarica molto breve) o normale (diverse ore); inoltre può essere presente la funzione di scarica completa della batteria prima di ricaricarla. Alcuni modelli di caricabatteria possiedono due alloggiamenti, per ricaricare altrettante batterie.

Infine ci sono i caricabatteria da automobile, che vanno collegati alla presa dell'accendisigari; in genre sono lenti e non danno una ricarica totale.

Cash display
Vedere AoC.

Categoria di emissione
Vedere Classe di potenza.

Cell-broadcast
Il gestore di rete può trasmettere informazioni di utilità sotto forma di messaggi testuali che compaiono sul display. Si applica solo ai GSM e vale per la cellula in cui si trova l'abbonato.

Cellulare
Sistema di telefonia senza fili via onde radio, basato su una rete di ricetrasmettitori opportunamente disposti per coprire il territorio con zone (celle) adiacenti.

Chiamata a vibrazione
Vedere Vibracall.

Chiamata vocale
Vedere Voice dialling

CID
Caller IDentification. Vedere CLI.

Classe di potenza
I telefonini GSM appartengono alla classe 4, a cui corrisponde una potenza fino a 2 watt. Gli apparecchi più grandi per automobili o trasportabili rientrano nella classe 2 (che corrisponde ad una potenza massima di 8 watt) o nella classe 1 (potenza fino a 10 watt).

CLI
Calling Line Identification. Tecnica che permette di visualizzare il numero del telefono chiamante; funziona solo in GSM e ISDN. CID e CLID sono sinonimi di CLI.

CLID
Calling Line IDentification. Vedere CLI.

CLIR
Calling Line Identification Restriction. Vedere CLR.

Clonazione
Operazione illegale che consiste nell'inserire in un secondo telefonino l'identificatore ESN corrispondente ad un telefonino analogico clonato, allo scopo di effettuare chiamate facendo pagare l'utente clonato.

CLR
Calling Line Restriction. Restrizione della tecnica CLI, in modo che il proprio numero non compaia sul display dell'apparecchio che riceve la chiamata.

Comando vocale
Vedere Voice dialling

Conversazione
Quando si effettua una conversazione, l'autonomia della batteria di un telefono cellulare si riduce notevolmente rispetto a quella che si ha nello stato di stand-by, ossia di attesa di una telefonata.

Copertura
Corrisponde all'area geografica al cui interno un telefono cellulare può ricevere ed effettuare chiamate. La copertura varia al cambiare del gestore di rete a cui si è abbonati.

Cordless
Senza fili. Il termine identifica i terminali casalinghi portatili o quelli appartenenti al nuovo sistema DECT.

Criptatura

Metodo di protezione delle comunicazioni applicato nel sistema GSM, per impedire l'intercettazione delle telefonate. Si tratta di un processo di codifica e decodifica cifrata, che necessita di apparecchiature specifiche e appositi algoritmi di trattamento dei pacchetti di dati digitali.

CT0 e CT1
CT0 (zero) rappresenta il primo standard analogico di telefoni cordless, affetto da numerose limitazioni. Ad esse si è cercato di porre rimedio col sistema CT1, le cui potenzialità restano tuttavia ancora ridotte rispetto al sistema digitale DECT.

DCS 1800
Vedere GSM 1800.

DCS 900
Vedere GSM 900.

DECT
Digital Enhanced Cordless Telecommunication. È il nuovo standard digitale per i telefoni cordless, con 120 canali distribuiti su 12 frequenze. La qualità è nettamente superiore agli standard CT0 e CT1.

Digitale
Si contrappone ad analogico ed identifica un sistema di ricetrasmissione dove vengono trasmessi dati sotto forma numerica (0 e 1 come nei computer). In natura i suoni vengono emessi e percepiti sotto forma analogica, per cui sono necessari processi di codifica (per passare da analogico a digitale in fase di trasmissione) e di decodifica (il passaggio inverso, per fornire il segnale riprodotto dall'auricolare). Il sistema digitale presenta vantaggi tecnici e pratici di vario tipo, come il migliore sfruttamento delle frequenze radio o l'impossibilità di clonare gli apparecchi e intercettare le telefonate.

Display
Visore che consente di leggere e scrivere dati alfanumerici; nei telefonini in genere è a cristalli liquidi LCD e può essere anche a colori. Il display può prevedere un numero maggiore o minore di righe.

Doppia banda
Vedere Dual Band.

Doppia modalità
Vedere Dual Mode.

DTMF
Dual Tone Multi Frequency, ossia trasmissione dei dati in multifrequenza. Questa tecnica consente di comunicare a distanza con segreterie telefoniche, banche dati, fax o altri dispositivi collegati ad un telefono cellulare. In futuro i toni DTMF serviranno per trasformare il telefonino in una specie di teledrin.

DTX
Discontinuous Transmission. Metodo di funzionamento di alcuni modelli di telefoni cellulari; consiste in una interruzione della trasmissione durante le pause del discorso, per risparmiare nel consumo della batteria. Per funzionare, il sistema deve essere supportato dal gestore del servizio.

Dual Band
Sono Dual Band quei telefonini che possono funzionare indifferentemente con le due frequenze di 900 e 1800 MHz; la prima viene utilizzata da Omnitel e TIM, mentre la seconda è riservata al terzo gestore Wind e a quelli che eventualmente arriveranno dopo.

Dual Mode
Alcuni telefoni sono Dual Mode, ossia possono funzionare secondo due standard differenti. Ci sono vari esempi: sono dual mode gli apparecchi GSM che funzionano anche come satellitari, oppure alcuni modelli d'oltreoceano che sono sia analogici che digitali, od anche gli apparecchi in doppia modalità GSM/DECT.

EFR
Enhanced Full Rate. Sistema di potenziamento della qualità della voce, per renderla di buona qualità anche nelle situazioni di segnale debole.

Ergonomia
Sono ergonomici quei telefonini che risultano non soltanto comodi da impugnare, ma anche agevoli e intuitivi nella disposizione dei tasti di comando, semplici nella costruzione dei menu, chiari nella lettura del display.

ERMES
Sistema di cercapersone su rete paneuropea. La maggior parte dei fornitori di servizio non la rende ancora disponibile.

ESN
Electronic Serial Number. Si tratta dell'identificatore numerico trasmesso da un telefonino analogico; esso serve all'identificazione univoca di ogni apparecchio da parte della stazione ricevente. Nel sistema GSM il numero analogo si chiama
E-TACS
Extended Total Access Communications System. È lo standard di ricetrasmissione utilizzato dai telefoni cellulari analogici.

ETSI
European Telecommunications Standards Institute. Sigla che contraddistingue l'organo responsabile degli standard telefonici validi in Europa.

FDN
Fixed Dialling Numbers. Funzione che permette di effettuare chiamate soltanto verso quei numeri che sono contenuti in un elenco

predefinito.

Feedback
Rimbombo o fischio che si innesca in un sistema di ricetrasmissione quando la propria voce viene captata anche dall'auricolare e va a sovrapporsi all'audio di ritorno dell'interlocutore. Avviene tipicamente nei sistemi viva voce delle automobili, ma spesso è apprezzabile anche nelle normali telefonate.

Flip
Sportellino messo a protezione della tastiera in alcuni modelli di telefoni cellulari. Può essere a cerniera (tipo più diffuso) o scorrevole; inoltre può essere attivo (aprendolo e chiudendolo si inizia e si conclude una conversazione) o passivo.

FLMPTS
Future Public Land Mobile Telecommunications System. Un probabile futuro standard di telefonia mobile, che l'International Telecommunications Union sta sviluppando in concorrenza col nuovo sistema europeo UMTS.

GAP
Generic Access Profile. Nel sistema DECT identifica i cordless che sono in grado di comunicare solo con la base e altri terminali ad essa collegati.

GPRS
General Packet Radio Service. Trasmissione di dati basata sulla loro scomposizione in pacchetti compressi; con questa tecnica si riesce a velocizzare lo scambio di dati su una rete cellulare digitale, arrivando fino a 115000 bit/secondo.

GSM
Global System for Mobile communication. È lo standard di ricetrasmissione utilizzato dai telefoni cellulari digitali.

GSM 900
Rete telefonica digitale GSM che lavora sulla frequenza di 900 MHz. È quella impiegata da Omnitel e TIM.

GSM 1800
Rete telefonica digitale GSM che lavora sulla frequenza di 1800 MHz. Viene utilizzata dal terzo gestore Wind e da quelli che eventualmente arriveranno dopo.

GSM 1900
Rete telefonica digitale GSM che lavora sulla frequenza di 1900 MHz. Viene utilizzata nell'America del Nord.

Hacker
Pirata. In informatica vengono contraddistinti con questo nome coloro che in un modo o in un altro contravvengono alle regole commerciali o tecniche imposte dal mercato. In telefonia gli hacker sono quelli che intercettano le telefonate di tipo analogico E-TACS, utilizzando un'apparecchiatura di scandaglio delle frequenze chiamata scanner. A maggior ragione, sono hacker anche coloro che clonano i telefonini analogici.

Hand-Over
Commutazione automatica che avviene quando il telefonino in movimento passa da una stazione ricetrasmittente ad un'altra. In genere l'utente non se ne accorge perché la comunicazione continua senza interruzioni.

Hardware
In inglese significa "ferramenta" e indica gli apparecchi in genere; viene usato in contrapposizione con tutto ciò che è software, ossia programmi per computer o altre apparecchiature altamente sofisticate.

Home Banking
Con questi termini viene indicata la possibilità di accedere a servizi bancari attraverso il telefono. Oltre che ad un apparecchio fisso, si può ricorrere anche a un telefono cellulare, purché sia dotato di una SIM Card avanzata (SIM Toolkit).

Hot-key
Tasto caldo. Viene chiamata in questo modo la possibilità di attivare una funzione su un telefonino semplicemente tenendo premuto un tasto. L'applicazione tipica è quella di far partire automaticamente la chiamata di un numero.

HSCSD
High Speed Circuit Switched Data. Tecnica di trasmissione dei dati in telefonia mobile, già in funzione in alcuni paesi. Serve per aumentare la velocità di trasmissione dai normali 9600 bit/secondo fino a 14400 bit/secondo.

Identificazione del chiamante
Vedere CLI.

IMEI
International Mobile Equipment Identity. È l'identificatore numerico trasmesso da un telefonino digitale; esso serve all'identificazione univoca di ogni apparecchio da parte della stazione ricevente. Nel sistema E-TACS il numero analogo si chiama ESN.

IMSI
International Mobile Subscriber Identity. Codice che serve per identificare un utente SIM a livello internazionale.

Interrogazione remota
Serve per ascoltare i messaggi registrati da una segreteria telefonica, consultandola a distanza.

IrDA
Infrared Data Association. Associazione di produttori che definisce lo standard per lo scambio di dati attraverso una porta a raggi

infrarossi. Col termine IrDA si intende comunemente la tecnologia stessa, che consente il collegamento tra apparecchiature differenti senza fare uso di cavi. Numerosi modelli di telefoni cellulari, computer portatili e stampanti fanno uso di porte IrDA.

ISDN
Integrated Service Digital Network. Sistema di telefonia via filo per trasmettere voce e dati di qualsiasi tipo (testi, immagini, filmati) ad alta velocità con tecnologia digitale.

ISO
International Standard Organization. Organismo internazionale che si occupa degli standard industriali. Nei telefonini ha stabilito le dimensioni e le caratteristiche delle schede SIM formato ISO.

ISPBX
ISdn Private Branch Exchange. Centralino telefonico di tipo ISDN. Vedere anche PABX e PBX.

ITU
International Telecommunications Union. Organismo americano che si occupa della definizione di nuovi standard telefonici.

Kit per auto
Indica l'accessorio dedicato all'installazione del cellulare sull'automobile. In genere prevede il collegamento alla batteria e agli altoparlanti.

LCD
Liquid Crystal Display. Piccolo schermo a cristalli liquidi, utilizzato nei telefoni cellulari per visualizzare numeri e tutti i dati alfanumerici necessari all'uso dell'apparecchio (nomi, voci di menu,...).

LED
Light Emitting Diode. Diodo che emette radiazioni luminose. Nei cellulari viene impiegato per segnalare alcuni parametri di funzionamento, ricorrendo a colori differenti e a diverse frequenze di intermittenza: la presenza di segnale, l'arrivo di una chiamata o lo scaricarsi della batteria.

Li-Ion
Batterie agli Ioni di Litio, la frontiera attualmente più avanzata nel campo dei telefonini. Sono piccole e leggere, danno una buona autonomia, non hanno problemi di memoria e si ricaricano in breve tempo.

Locazione di memoria
Parte della rubrica dove viene immagazzinato un numero telefonico e il nome ad esso associato (dati alfanumerici).

Memoria
Vedere Locazione di memoria.

Memoria One-touch
Vedere Hot-key.

Menu
Sistema di voci organizzate che compaiono sul display, per rendere disponibili le varie funzionalità dell'apparecchio telefonico.

Microcellula
Vedere Cell-broadcast.

MMM
Mobile Media Mode. Tecnologia sviluppata per consentire ai cellulari di navigare in Internet. Vedere anche WAP.

Modem
Modulation demodulation. Apparecchio che consente di inviare dati digitali lungo una linea telefonica. Da una parte deve essere collegato a un computer, dall'altra ad una rete telefonica a filo o via radio.

Mute
Funzione che permette di escludere il microfono del proprio telefonino durante una conversazione.

NAM
Nei cellulari E-TACS nuovi indica la procedura di inizializzazione, con l'inserimento dei dati del possessore.

NiCd
Identifica le batterie al Nichel-Cadmio, che sono state le prime ad essere utilizzate sui telefonini. Sono più grandi e pesanti di quelle venute dopo (NiMh e LiIon), danno un'autonomia limitata e soffrono anche dell'effetto memoria.

NiMh
Batterie al Nichel-Metalidrato, che danno una buona autonomia. Tuttavia cominciano a deperire dopo circa 300 cicli di ricarica.

Numero caldo
Vedere Hot-key.

OGM
La sigla identifica il messaggio emesso da una segreteria telefonica o da una casella vocale, per invitare l'interlocutore a lasciare la sua comunicazione.

One-touch

Vedere Hot-key.

PABX
Private Automatic Branch Exchange. Identifica le centrali automatiche presenti in molti uffici, a derivazione o distribuzione multipla.

Pay-as-you-go
Vedere Schede prepagate.

PBX
Private Branch Exchange. Centrale telefonica multilinea simile alla PABX, ma senza distribuzione automatica.

PC Card
Scheda che permette di effettuare il collegamento tra un computer portatile e un telefonino GSM, al fine di scambiare dati o fax, oppure per collegamenti a Internet. In genere la PC Card è composta da un modem.

PCMCIA
Personal Computer Memory Card International Association. Scheda per computer portatili, utilizzata per inserire un modem o altri dispositivi accessori. È sinonimo di PC Card.

PCN
Personal Communication Network. Rete per comunicazioni personali, sinonimo di GSM 1800.

PCS
Personal Communication System. Sistema per comunicazioni personali, sinonimo di GSM 1900, utilizzato in Nord America.

PCX
Private Communication Exchange. Sistema di comunicazione telefonica integrato a livello aziendale.

PDA
Personal Digital Assistant. Agende elettroniche sofisticate, con prestazioni che sfiorano quelle di un computer portatile. Un numero sempre maggiore di telefoni cellulari svolgono funzioni di tipo PDA.

PIN
Personal Identification Number. Numero utilizzato per bloccare l'uso della SIM Card; serve per proteggerne l'uso indebito. L'utente ha la possibilità di modificare il codice PIN, formato da quattro cifre. In molti casi sono disponibili due codici, contraddistinti dalle sigle PIN1 e PIN2.

Pirata
Vedere Hacker.

Plug-in
Uno dei due formati delle SIM Card che vanno inserite nei telefonini GSM. Il tipo plug-in è molto piccolo e viene denominato anche "mini".

PMR
Private Mobile Radio. Radio ricetrasmittenti utilizzate da taxi e simili. Utilizzano onde radio di frequenze prestabilite, senza passare attraverso fornitori di servizio telefonico.

Portatile
Identifica un telefono cellulare di dimensioni molto piccole e tascabili. Si contrappone ai modelli trasportabili o veicolari.

Protocol ID
Protocol IDentification. È il codice che identifica il tipo di messaggio nel sistema GSM.

PSTN
Public Switched Telephone Network, rete telefonica pubblica commutata. Indica la normale rete telefonica fissa, collegata via cavo.

PUK
Personal Unblocking Key. Con questa sigla viene indicato il codice di sblocco fornito dal gestore di rete, qualora si sbagli per tre volte consecutive la digitazione del codice PIN. Quando sono disponibili due codici PIN1 e PIN2, ci sono i corrispondenti PUK1 e PUK2. I codici PUK, formati da otto cifre, non sono modificabili dall'utente.

RF
Radio Frequency. Indica il segnale in radio frequenza che intercorre tra la stazione fissa e il telefono cellulare ad essa collegato.

Roaming
Questo termine indica la possibilità di usare il telefono cellulare all'estero, servendosi di gestori locali che devono essere convenzionati con quello a cui si è abbonati in Italia.

RS-232
Porta seriale dei computer. Talvolta è presente su un apparecchio cellulare, per collegarlo al computer e scambiare dati con esso.

Rubrica
Funzionalità dei telefoni cellulari, dedicata alla memorizzazione e alla consultazione dei numeri telefonici inseriti nelle locazioni di memoria.

Scanner

Apparecchio radio speciale che è in grado di scandagliare uno spettro molto ampio di frequenze; viene utilizzato dagli hacker per intercettare numerosi tipi di comunicazioni su bande riservate, come polizia, traffico aereo, cellulari E-TACS o altri generi di servizi via radio.

Schede prepagate
Consentono di effettuare telefonate senza dovere stipulare un contratto di abbonamento con canone. Internazionalmente sono note col nome Pay-as-you-go (paghi quando telefoni).

Scrambling
Tecnica di crittazione di un segnale digitale per impedirne l'intercettazione. Viene utilizzato dai gestori di rete per rendere sicure le comunicazioni GSM.

Scratch pad
Possibilità di memorizzare un numero telefonico in una memoria temporanea, nel corso di una conversazione. Utile per appuntarsi un numero al volo, trasferendolo successivamente in rubrica.

SDN
Service Dialling Numbers. Insieme di numeri di servizio che possono essere spediti dal gestore della rete ad uso dell'utente. Si tratta di una funzionalità di tipo dinamico, la cui disponibilità dipende la gestore.

Short Message Service
Vedere SMS.

SIM
Subscriber Identity Module. Con SIM Card si identifica la scheda che sta alla base del funzionamento di un telefonino GSM; essa contiene i dati dell'abbonato. Esiste in due formati: ISO (simile ad una carta di credito) e plug-in (della grandezza di un francobollo). Ogni SIM prevede codici PIN e PUK di protezione.

SIM Toolkit
Con questo nome vengono identificate le SIM Card di ultima generazione, che rendono disponibili servizi interattivi avanzati, come la prenotazione di viaggi o l'interfacciamento con la propria banca (Home Banking).

SMS
Short Message Service. Possibilità di trasmettere o ricevere brevi messaggi alfanumerici, composti mediante la tastiera del telefonino. Questi messaggi sono soltanto in forma scritta e vengono visualizzati sul display del ricevente.

Soft-key
Indica un tasto la cui funzione varia col variare della situazione in cui si trova l'apparecchio in quel momento. La funzione via via svolta viene indicata sul display. Si tratta di un metodo molto pratico per ridurre il numero di pulsanti.

Software
In campo informatico indica l'insieme dei programmi che fanno funzionare un computer. Nella telefonia mobile il software serve per gestire le funzionalità di un telefonino, al cui interno ci sono microprocessori programmabili.

Sottomenu
Un sistema di menu ben concepito raggruppa le funzionalità simili in voci di sottomenu, per facilitare la gestione delle opzioni.

Standby
Indica lo stato di attesa di un telefonino acceso. Generalmente viene utilizzato per indicare il numero di ore durante le quali è possibile effettuare o ricevere chiamate con una batteria completamente carica. In conversazione tale autonomia si riduce notevolmente.

Stazioni radio base
Sono le postazioni fisse che forniscono la copertura del territorio in un sistema di telefonia cellulare.

Suoneria a vibrazione
Vedere Vibracall.

Supertwist
Questo termine identifica la tecnologia dei display che sono più grandi e leggibili di quelli normali. In tal modo aumenta il numero delle informazioni alfanumeriche visualizzate.

T9
Tecnologia per l'immissione di messaggi mediante la tastiera del telefonino, avente lo scopo di evitare la pressione ripetuta dei tasti per ricercare la lettera giusta tra quelle associate ad ogni tasto. Le lettere digitate vengono analizzate e confrontate con un database linguistico, per fornire la parola corretta premendo una sola volta i vari tasti letterali (come si farebbe su una normale tastiera per computer).

TACS
Vedere E-TACS

Touch panel
Display sensibile al tocco. Alcuni telefonini o PDA possiedono questo tipo di visore, in cui si scelgono le opzioni toccando con un dito o con l'apposita penna. Nei PDA più avanzati è presente anche il riconoscimento della scrittura fatta a mano libera sul display.

Touch screen
Vedere Touch panel

Trasportabile
Telefono mobile di dimensioni nettamente superiori a quelle di un moderno telefonino portatile. In genere si ricorre a questi modelli per avere a disposizione una maggiore potenza di emissione e una grande autonomia di batterie.

Trickle Charge
Carica di mantenimento. Un buon caricabatteria eroga questa carica ridotta quando la batteria è già completamente carica, per non rovinarla.

UMTS
Universal Mobile Telecommunications Standard. Sistema di comunicazione ancora in fase di sviluppo; è basato su linee dedicate ad alta velocità, per trasmettere grandi quantità di dati. Sarà possibile trasmettere immagini, comprese quelle in movimento; il punto d'arrivo di questo standard prevede servizi avanzati quali Internet, videconferenze, cortometraggi e tv cellulare.

Veicolare
Telefono cellulare installato a bordo di una automobile; è collegato ad una antenna esterna e alla batteria della macchina e possiede in genere una potenza superiore a quella di un telefonino. Spesso è possibile trasformare un telefono veicolare in un trasportabile.

Vibracall
Dispositivo che fa vibrare un telefonino quando arriva una chiamata. Serve per disinserire la normale suoneria nei casi in cui può dare fastidio o creare imbarazzo. Il vibracall può essere inserito all'interno dell'apparecchio, oppure in una batteria apposita.

Vibrazione
Vedere Vibracall

Vivavoce
Sistema per utilizzare il telefonino in automobile senza dovere tenere l'apparecchio accostato all'orecchio. Quasi tutti i modelli portatili possono essere trasformati in veicolari acquistando l'apposito kit. Chi vuole usare il telefono in macchina deve averlo veicolare per legge.

Visualizzazione del chiamante
Vedere CLI.

Voice dialling
Possibilità di effettuare direttamente una chiamata mediante comando vocale. I cellulari che offrono questa funzione prevedono un'apposita procedura per la registrazione in memoria dei diversi comandi vocali.

Voice memo
Capacità che hanno alcuni telefoni cellulari di registrare appunti sonori durante il corso di una conversazione. La durata della registrazione è variabile da modello a modello e in genere non supera uno o due minuti. La registrazione può essere successivamente riascoltata e cancellata.

Voice note
Vedere Voice memo.

WAE
Wireless Application Environment. Ambiente di sviluppo che consente di realizzare un browser che soddisfi le specifiche WAP; il browser serve per collegare un telefono cellulare o altri dispositivi (come PDA o cercapersone) alla rete Internet.

WAP
Wireless Application Protocol. Standard che stabilisce le modalità di comunicazione tra telefoni cellulari e Internet o altre applicazioni su computer. Vedere anche MMM.

WML
Wireless Markup Language. Linguaggio con cui sono scritte le pagine Internet da visualizzare coi telefonini mediante il protocollo WAP.
