SECURITY DIVISION
Security & Intelligence Services

Prodotto CryptoMobile per vendita e affitto

1 - PREMESSE

1.1 - Anonimità
Nascondere la propria identità può essere una scelta, per legittime ragioni di privacy e, in alcune occasioni, per sicurezza personale.
Internet ha consentito la divulgazione e la pubblicazione di informazioni in forma parzialmente anonima. Tuttavia, la diffusione delle comunicazioni via Internet ha spinto governi e multinazionali a sviluppare metodi di sorveglianza senza precedenti: Echelon e Carnivore sono soltanto alcuni esempi.

La *privacy* si traduce spesso nella capacità di di impedire che le informazioni che ci riguardano diventino note ad altri, inclusi organizzazioni ed enti, qualora il soggetto non abbia volontariamente scelto di fornirle.

1.2 - Sistema crypto
E' un sistema che include testo in chiaro, testo cifrato e delle chiavi di codifica e decodifica. Un elemento essenziale per determinare la sicurezza di un sistema di protezione delle informazioni, quali ad esempio Enigma, e' la pubblicazione dell'algoritmo di cifratura: la conoscenza di tale algoritmo e' l'unico metodo per poter analizzare le informazioni criptate e poterle eventualmente decifrare. In alcune nazioni, ad esempio gli USA, le uniche soluzioni di codifica permesse sono quelle che prevedono l'accesso alle chiavi di decodifica, per poter intervenire e leggere i dati nascosti.

1.3 - La codifica
Vengono scambiate le chiavi di codifica e la chiave simmetrica, valida solo per questa unica telefonata, viene generata dal telefono chiamante ed inviata a quello chiamato, che la decodificherà mediante la propria chiave segreta. Questa chiave segreta è invisibile agli altri apparati. Da questo punto in avanti, entrambi gli apparati codificano tutti i segnali in uscita, con la chiave ed invieranno i dati codificati ai partecipanti alla conversazione. Questa chiave è unicamente disponibile per una conversazione, ed in occasione di una prossima conversazione ne verrà creata una nuova. Alla fine della conversazione, la chiave simmetrica sara' eliminata e non sara' mai più utilizzata. Questo aumenta ancor di piu' la sicurezza delle conversazioni, in entrambe le direzioni.. Una volta chiusa la chiamata, anche la codifica della conversazione viene ovviamente terminata.

1.4 - L'IMEI
Ogni telefono e' dotato di un numero IMEI, (International Mobile Equipment Identity) un numero di 15 cifre che è unico ed è costituito da un codiche seriale che identifica il prodotto più altri dati. E' sempre possibile modificare il numero IMEI di un apparecchio. L'IMSI viene assegnato dal gestore. Se richiesto dalla stazione cellulare in cui si trova, la SIM invia il proprio IMSI invece del TMSI (Temporal Mobile Subscriber Identity) per permettere alla stazione cellulare la sua identificazione. Parimenti, il telefono (l'hardware) invia il proprio codice, l'IMEI (International Mobile Equipment Identity)

1.5 - L'IMSI

Ogni Sim card GSM e' dotata di un numero IMSI, (International Mobile Subscriber Identity) un numero di 15 cifre che è unico ed è costituito da un codiche che identifica la nazione, il gestore, l'abbonato ed altri dati. L'IMSI viene assegnato dal gestore. Se richiesto dalla stazione cellulare in cui si trova, la SIM invia il proprio IMSI invece del TMSI (Temporal Mobile Subscriber Identity) per permettere alla stazione cellulare la sua identificazione. Parimenti, il telefono (l'hardware) invia il proprio codice, l'IMEI (International Mobile Equipment Identity)

1.6 - Man in the Middle

La definizione di man in the middle attack (MiM) indica un attacco in cui chi lo genera è in grado di leggere e modificare a piacimento messaggi e contenuti senza che le due estremità della conversazione se ne accorgano.

1.7 - Intercettazione tramite un cattura IMSI

Una volta simulata la presenza di una stazione cellulare con una potenza superiore alle altre,il telefono cellulare da "ascoltare" risponderà alle richieste di ascolto della stazione mettendo a disposizione della finta cellula tutti i propri dati: IMSI, IMEI, TMSI ed altri. A questo punto, la codifica standard del GSM viene spenta tramite apposito comando generato dalla finta stazione cellulare: tutte le conversazioni saranno in chiaro e potranno essere semplicemente ascoltate e/o registrate. Contemporaneamente, il cattura IMSI inviarà la chiamata alla vera stazione cellulare (quella del gestore) in modo che la chiamata possa effettivamente andare a destinazione. Si puo' monitorare tale azione furtiva, ma non prevenirla.

2 - CRITTAZIONE

2.1 - Il sistema GSM ha una codifica insufficiente.

Il GSM offre una semplicissima forma di codifica per la protezione delle chiamate, chiamata "stream encryption method A5", un protocollo semplicissimo, che puo' venir decodificato molto semplicemente, usando un PC, mediante i metodi Biryukow, Schamir, Wagner. Una chiamata che viaggia su reti GSM e' praticamente sempre leggibile, anche perchè poi se finisce nella rete normale PSTN (la normale rete telefonica) la protezione decade e la chiamata passa in chiaro. Un altro metodo per leggere le telefonate è basato sulla "cattura" dell'IMSI: in generale, ogni telefono GSM cerca il collegamento alla cella con il segnale più potente tra quelli disponibili. Il "cattura IMSI", l'apparato che consente l'intercettazione delle chiamate GSM, simula l'attività di una stazione cellulare (ci sono sempre 10-20 stazioni cellulari tra cui il telefono sceglie quella più potente) ai telefoni presenti nel suo raggio d'azione, che rispondono così alle sue richieste. Il cattura IMSI intercetta così tutte le chiamate e le re-indirizza (senza che i proprietari se ne accorgano) verso la vera stazione cellulare. Allo stesso tempo, invierà le chiamate identificate tramite identificazione dell'IMEI e dell'IMSI verso una stazione pirata d'ascolto, tramite una connessione separata ed invisibile.

In aggiunta a quanto sopra descritto, un semplice comando contenuto nello standard GSM può eliminare la codifica standard prevista dal GSM stesso, permettendo così un ascolto del contenuto delle conversazioni in tempo reale. Si possono acquistare nei negozi specializzati appositi strumenti capaci di generare tali comandi. L'uso di questi strumenti non e' consentito dall'autorità delle Telecomunicazioni e può anche essere pericoloso poichè i segnali emessi possono disturbare notevolmente le frequenze della rete GSM interessata.

2.2 - Cos'è un crypto-algoritmo?
Per poter proteggere delle conversazioni confidenziali, e' necessario utilizzare delle funzioni matematiche che rendano le proprie informazioni il più possibile difficili da decifrare: queste funzioni matematiche sono definite algoritmi di codifica. Generalmente vengono usati due algoritmi, uno per cifrare ed uno per decodificare. Nelle moderne tecniche di cifratura, gli algoritmi sono visibili, mentre la loro sicurezza è basata solamente sull'utilizzo delle chiavi di codifica. Il mancato accesso o possesso di queste chiavi rende impossibile la decodifica delle informazioni. .

2.3 - Cos'è una chiave?
Una chiave è una catena di caratteri generata casualmente e che può essere trasmessa elettronicamente. Più lunga la catena, maggiore la sicurezza della chiave. Una chiave permette o nega l'accesso al messaggio scambiato. Così come con le chiavi utilizzate per poter proteggerte le nostre case, le nostre macchine, non esiste una chiave sicura al 100%. L'unica soluzione sarebbe quella di avere una serratura ed una chiave che ad ogni uso cambiano forma e dimensione, per poter essere sempre sicuri che nessuno le possa duplicare e cosi' entrare in casa/rubare l'auto.

2.4 - La procedura simmetrica
Nel caso della cifratura simmetrica, l'inviante delle informazioni ed il ricevente usano la stessa chiave segreta. I vantaggi sono riassumibili in rapidità di esecuzione delle operazioni e nessuna gestione delle chiavi di cifratura, mentre lo svantaggio e' che chiunque può accedere alla chiave. La perdita della chiave di cifratra rende le informazioni praticemente disponibili a chi la trova. Può inoltre essere anche un problema il dover trasferire la chiave di cifratura ai propri contatti, che devono cioè riceverla per poter accedere alle informazioni riservate. Esistono inolte sul mercato anche alcuni telefoni che contengono al proprio interno una chiave di cifrtura poichè usano tutti la stessa chiave, i dati trasferiti possono venir letti/ascoltati semplicemente utilizzando un apparato dello stesso modello e marca. Questa chiave AES256 usa l'algoritmo ufficiale del NIST a 256 bit ed è considerato inattaccabile.

2.5 - La procedure asimmetrica
Nel caso delle procedure di cifratura asimmetriche, esiste una coppia di chiavi per ogni partecipante al processo. Una delle due chiavi di tale coppia e' la cosidetta chiave segreta privata del proprietario dell'apparato, che viene sempre mantenuta segreta, che viene utilizzata solo dal proprietario, e che non deve essere trasferita ad altri. La seconda chiave della coppia e' pubblica ed è a disposizione ai partecipanti alla comunicazione, come se fosse in un elenco (e' cioe' possibile anche gestire una conversazione tra più utenti, sempre in sicurezza e sotto cifratura). La cifratura viene stabilita usando la chiave pubblica (della coppia di chiavi disponibili). La decodifica del messaggio inviato e' possibile utilizzando la chiave privata (della coppia di chiavi disponibili). Anche conoscendo la chiave pubblica, non si porta' ridecodificare il messaggio poichè la chiave privata non è disponibile nè può essere calcolata o rigenerata. pertanto, solo il destinatario del messaggio può in effetti leggere e decifrare il testo cifrato, testo cifrato che non puo' ovviamente essere manipolato, e letto da nessuno. L'unicità della coppia di chiavi permette anche il riconoscimento unico dei partner autorizzati ad entrare in possesso delle informazioni cifrate. Questa chiave utilizza addirittura 1024 bit di codifica sarebbero necessari 70 miliardi di anni per decifrarla.

I vantaggi della cifratura asimmetrica sono un'assoluta segretezza delle informazioni, la mancata presenza di una chiave scambiata tra i partecipanti per poter codificare/decodificare le informazioni e l'assoluta sicurezza nell'identificazione dei partecipanti alle sessioni di scambio dei dati. Lo svantaggio consiste principalmente nel superiore costo degli apparati dovuto alla creazione ed alla gestione delle chiavi pubbliche e private ed una inferiore velocità di decodifica.

2.6 - La combinazione di procedure simmetriche e asimmetriche (procedure ibride)
La garanzia più elevata di sicurezza si raggiunge mediante l'uso combinato di teniche simmetriche ed asimmetriche. Viene cioè creata una chiave, utilizzabile solo una volta, simmetrica valida solo per una comunicazione/una telefonata che viene trasnessa al ricevente, mediante una procedura asimmetrica. La cifratura dei dati da scambiare viene eseguita utilizzando la chiave simmetrica conosciuta solo dai due apparati correlati. Quest'approccio permette un'elevata velocità di codifica ed elimina gli svantaggi delle procedure simmetriche mantenendo però i vantaggi delle procedure asimmetriche.

2.7 - La chiave di cifratura pubblica può essere intercettata, ma non è possibile utilizzarla per decifrare la conversazione/il messaggio. Non è possible per la società che ha scritto il software decifrare le conversazioni eventualmente registrate da terze parti poiché ogni chiave di cifratura viene distrutta al temine della chiamata.

3 – IL PRODOTTO

3.1 - Qualità della chiamata codificata.
Il metodo di compressione utilizzato nella fase della codifica dei suoni in uscita e' il più modermo attualmente sul mercato: pertanto la qualita' non è peggiore di quella della maggior parte dei telefoni GSM presenti sul mercato. La chiamata codificata viene istradata sulla linea dati dell'apparato, l'unica che permette il passaggio della quantità di dati necessari a garantire la sicurezza della conversazione. La linea dati richiede una maggiore stabilità del segnale, pertanto potrebbe essere sconveniente muoversi ad alta velocità od in zone in cui il segnale della portante GSM e' inferiore al 15/20%.

3.2 – Posso selezionare il destinatario della chiamata dalla mia lista di contatti
Se la funzione è abilitata nel software, appare un menu, con i tuoi contatti: clicca e tieni premuto su CONTATTI per selezionare SECURECALL call per aprire la chiamata direttamente dalla schermata dei contatti.

3.3 - Entrambi gli utilizzatori devono avere il software installato per eseguire una chiamata sicura.
E’ necessario che l'identico software sia installato ad entrambe le estremità della conversazione. Posso ancor aeseguire chiamate normali non protette verso utenti che non abbiamo installato il software. Solo la cifratura protegge dall'attacco di terze parti, man-in-the-middle, che cerchino di intromettersi nella conversazione grazie agli speciali algoritmi utilizzati ed al modulo di verifica dell'identità.

3.4 – Assenza di ECO
La qualità della conversazione è facilmente testabile provando i prodotti degli altri concorrenti. Tra i più famosi è disponibile nel sito di SecureGSM il software gratuito a bassa crittazione (insicuro) per testare il prodotto. Sinoteràchelacomunicazione non è fluida, ci sono echi e ritardi eccessivi e fruscii che disturbano la conversazione che rendono il prodotto praticamente inutilizzabile. Il nostro prodotto ha una qualità simile a quella di un telefono GSM comune.