SATSEC 1400

Secure Wireless telecommunications with Thuraya, Globalstar Satellite Phoones

Se vuoi sicurezza nelle tue conversazioni con un telefono satellitare
Thuraya o Globalstar non hai soluzione più appropriata.

Lo strumento proposto da Speeka e' il mezzo ideale per raggiungere la sicurezza delle tue conversazioni.

Molto piccolo, compatto, facilmente utilizzabile su telefoni satellitari Thuraya e Globalstar , il SatSec 1400 si collega semplicemente alla connessione dati disponibile con il telefono satellitare. E' dotato di alimentazione autonoma a batterie per operatività "on the road" in lughi remoti; e' però anche fornito di di apposito alimentatore da rete per permettere un utilizzo prolungato in caso di necessità.

Il SatSec 1400 e' dotato di un apposita cuffia auricolare per la gestione delle chiamate in totale sicurezza.

Una volta connesso ad apparati telefonici satellitari Globalstar o Thuraya, o anche a telefoni cellulari, il SatSec-1400 fornisce la massima sicurezza nella cifratura della voce.
La cifratura viene gestita selezionando il canale dati dell'apparato satellitare, sul quale la comunicazione viene smistata.

Ovviamente, la velocita' di trasmissione è limitata dalla larghezza di banda disponibile, che nel caso di Thuraya e Globalstar e' di 9600bps, una larghezza di banda che assicura un'ottima qualita' di ascolto.
Il SatSec-1440 utilizza gli algoritmi di cifratura Citadel CCX, sviluppato da Harris Corporation, per maggior sicurezza della protezione.

Per l'effettuazione di chiamate criptate e' ovviamente necessario utilizzare una coppia di apparati ad entrambe le estremita' della conversazione.

THURAYA

Globalstar

SPECIFICHE TECNICHE

Algoritmo di cifratura	Harris CITADELTM CCX
Chiave di cifratura telefonica	3.4 x 10^{38} combinazioni (chiave a 128-bit)
Minima velcoità di comunicazione	2400bps throughput
Connessione con telefono satellitare	Connettore DB-9 Seriale
Alimentazione	90-240 Volts A/C 50 – 60 Hz
Peso	50 grammi
Batteria	Batteria Ioni di Litio, fino a 6 ore di conversazione. La conversazione cifrata puo' anche avvenire durante la ricarica della batteria.
Consumo elettrico	6 Watts
Dimensioni	5" D x 2.2" W x .375" H (127mm D x 56mm W x 10mm H)

CARATTERISTICHE DELLE PROCEDURE DI CIFRATURA

Gli algoritmi utilizzati sono di tipo simmetrico: richiedono sempre la stessa chiave di codifica ad entrambe le estremità della conversazione. Le chiavi non vengono trasmesse in chiaro, poichè potrebbero essere intercettate compromettendo così la sicurezza della conversazione.

Il Citadel™ CCX utilizza chiavi a 128 bit. Il design tecnico del prodotto consente la conversazione cifrata solo tra due apparati, evitando cosi' che qualsiasi tipo di ascolto non autorizzato possa essere possibile, in ogni momento.

Speeka s.r.l. • Via Carlo Pisacane 42 • 20129 Milano • Italy • clienti@speeka.com • www.speeka.com

Tel. + (39) 02.295.14.666 • Fax + (39) 02.295.34.639 • P.IVA 10351030159

La procedura utilizzata per creare le chiavi segrete di codifica e' chiamato Diffie-Hellman Key Agreement: questa procedura permette a due utenti di creare e gestire le chiavi segrete di codifica necessarie per la conversaizone sulla base dei seguenti principi:

a) All'inizio di ogni telefonata, ogni SatSec 1400 genera un numero privato, casuale, che viene mantenuto segreto all'interno del SatSec 1400 stesso. La procedura matematica utilizzata viene definita **"funzione ad una via"**, che ha come input il numero privato casuale generato all'inizio della chiamata e come output un secondo numero definito chiave pubblica. Il principio della cifratura si puo' paragonare al macinacaffè: una volta che i chicchi sono stati triturati, non possono più essere ricomposti. Quindi, una volta che viene generata la chiave pubblica, non si puo' tornare indietro e reperire la chiave privata.
b) Nel corso della telefonata vengono poi scambiate le chiavi pubbliche. Chiunque voglia ascoltare la telefonata puo' intercettare le chiavi pubbliche, senza problemi, mentre invece le chiavi private casuali sono mantenute segrete all'interno del SatSec 1400 e non sono trasmesse all'esterno.

Una volta che le chiavi pubbliche sono state scambiate, un secondo processo matematico viene iniziato in entrambi gli apparati che abbinano la propria chiave privata con quella dell'altro apparato, creando un terzo numero definito chiave di sessione. Il processo matematico funziona in modo tale che le chiavi di sessione generate da entrambe le parti siano identiche e che il numero sia utilizzato come la chiave di cifratura per l'algoritmo di cifratura.
Una terza parte che volesse eventualmente ascoltare la conversazione potrebbe aver accesso alle chiavi pubbliche mentre vengono scambiate, ma non alle chiavi private, che sono custodite all'interno del SatSec 1400: in questo modo non è possibile ricreare la chiave di sessione necessaria per accedere alla conversazione.
Il Satsec 1400 garantisce la confidenzialità generando sempre chiavi nuove, private e pubbliche, all'inizio di ogni sessione di cifratura (ogni telefonata).

The Citadel TM Advantage

L'algoritmo Citadel™ e' stato sviluppato da Harris Corporation, uno dei leader mondiali nel settore della cifratura per oltre 40 anni. Il Citadel è un algoritmo di alta qualità utilizzato per proteggere le comunicazioni dei militari e degli apparati governativi. Il Citadel puo' essere anche personalizzato per scopi particolari, garantendo così autonomia di funzionamento e facilità di aggiornamento dello standard della sicurezza senza dover cambiare l'equipaggiamento hardware.
Di seguito, vengono elencati I vantaggi dell'algoritmo Citadel, contro altri algoritmi commerciali quali ad esempio il DES ed il 3DES.

1) L'algoritmo Citadel non e' rilasciato pubblicamente: questa caratteristica lo protegge autonomanente da attacchi organizzati, come quelli che sono stati condotti contro il DES ed il 3DES.
2) L'algoritmo Citadel, per la sua struttura e definizione e la sua scarsa efficienza software, non si presta ad attacchi paralleli anche da parte di reti di computer collegati tra di loro per aumentare la capacità di calcolo. Sono invece famosi questi attacchi portati con successo contro il DES ed il 3 DES.
3) 3) L'algoritmo Citadel e' utilizzato da organizzazioni governative e militari in tutto il mondo, ed è implementato anche nell'Harris Secure Voice and Data Unit (SVDU) e nelle radio tattiche Harris Falcon II HF/VHF, ad esempio.
4) In applicazioni militari, gli algoritmi di cifratura vengono cambiati od aggiornati in continuazione per vari motivi, tra cui separazione dei network (autonomia della sicurezza), interoperabilità, o per prevenire l'intromissione esterna nei propri sistemi, qualora l'equipaggiamento venga perso o rubato. L'algoritmo Citadel permette, senza dover modificare l'equipaggiamento, un aggiornamento continuo e costante od anche una personalizzazione delle caratteristiche di cifratura.
5) L'algoritmo Citadel non ha chiavi deboli come invece ha il DES: per chiave debole si intende una chiave che ha un numero piu' basso di ""key bits""effettivi rispetto alla lunghezza fisica della chiave stessa.
6) Gli algoritmi DES e 3DES sono vulnerabili alle criptoanalisi lineari e differenziali.
7) L'algoritmo 3DES raggiunge la lunghezza di chiave operativa attraverso passaggi multipli tramite una porta DES: e' pertanto vulnerabile agli attacchi diretti, definiti "meet in the middle attack". L'algoritmo Citadel raggiunge invece la lungheza di chiave in un singolo passaggio ed in una singola operazione: non è pertanto vulnerabile agli attacchi di tipo "meet in the middle attack".
8) Gli algoritmi DES e 3DES sono algoritmi commerciali e sono disegnati da un punto di vista commerciale, per la protezione contro attacchi che si possono definire commerciali. La famigli degli algoritmi Citadel è invece concepita e disegnata per scopi militari, per la protezione di interessi militari, governativi e quindi per la protezione contro attacchi più sofisticati, quelli al più alto livello. Grazie a questi concetti, l'algoritmo Citadel protegge e' è completamente sicuro contro tutti gli attacchi di criptoanalisi, indipendentemente dalle risorse disponibili a chi volesse eventualmente penetrare nei sistemi di protezione. Non sono pertanto conosciute delle vulnerabilità dell'algoritmo Citadel alle moderne e conosciute tecniche di lettura di informazioni cifrate. Nel caso di algoritmi come il Des ed il 3DES, invece, sono presenti varie tecniche di lettura, commercialmente disponibili: algoritmi commerciali come il DES ed il 3DES sono completamente inappropriati per qualsiasi tipo di applicazione militare e per qualsiasi tipo di informazione che deve essere protetta ad ogni costo da intrusioni esterne.

RIEPILOGO DEI VANTAGGI DEL SATSEC 1400

Soluzioni di protezione hardware delle chiavi di cifratura; gli algoritmi di cifratura hardware sono a prova di lettura; l'hardware è immune ad attacchi via internet; non sono necessarie passwords e nomi utente per accedere ai processi di cifratura; le soluzioni hardware di cifratura contegono dei generatori casuali di rumore ed i numeri generati sono veramente casuali; la generazione delle chiavi di cifratura non può venir alterata da hackers; le soluzione hardware non lasciano residui software nella memoria degli apparati;