

CELLULARI LE NOVITÀ ANTI-INTERCETTAZIONE

Criptofonino di massa

Caspertech taglia i prezzi.

Basta un tasto e partono i codici per criptare la telefonata

Rendere il criptofonino un prodotto di massa (o quasi), così che anche un normale avvocato, notaio o bancario possa parlare con il cellulare senza tema di essere intercettato. È questo adesso lo scopo di Caspertech, azienda torinese che produce software in grado di criptare le chiamate: ha lanciato la settimana scorsa Easy Cryptech, a 999 euro, Iva inclusa. Prezzo che comprende anche il palmare-smartphone dove il software è preinstallato (modelli Qtek 8300, Htc S620 e S710, a scelta dell'utente; per l'HTC Touch il prezzo sale a 1.049 euro). «Abbiamo deciso che era il momento di dare una svolta a questo mercato: adesso anche il cittadino comune può permettersi la privacy, mentre prima il nostro target, con un criptofonino più complesso, che costa 2.400 euro, erano solo gli alti dirigenti, i militari, gli ambasciatori», dice Ferdinando Peroglio, direttore commerciale di Caspertech. Il mercato comincia a rispondere: «Da quando abbiamo accettato i primi ordini dell'Easy Cryptech, un mese fa, abbiamo venduto decine di migliaia di prodotti, contro le migliaia al mese del periodo precedente».

La nuova strategia si serve anche di un accordo con il distributore E-Motion, «a oggi 53 punti vendita in Italia; circa cento entro fine anno». E-Motion ha già siglato, a riguardo, una convenzione con il Parlamento italiano. I primi ad acquistare il prodotto non sono stati però politici, ma «aziende finanziarie, para bancarie e quelle che spendono molto in ricerca: studi legali e notari». Caspertech cerca di costruire un prodotto di massa anche semplificandone l'utilizzo. «Adesso basta che l'utente selezioni il contatto e prema il tasto verde: la chiamata sarà criptata in automatico. Ovviamente a tal scopo è necessario che anche l'altro interlocutore usi un nostro terminale». Il criptofonino Caspertech più costoso, invece, permette anche di inserire a mano la chiave da usare per criptare la chiamata. «La funzione manuale torna comoda per i militari, che vogliono tenere sotto controllo il processo ed essere in grado di richiedere ai sottoposti la consegna delle chiavi scelti».

Easy Cryptech ha anche una funzione per criptare gli sms: anche in questo caso, il sistema funziona solo se il destinatario ha un altro criptofonino Caspertech. Con gli sms, però, l'utente deve scegliere una chiave e digitarla manualmente nel software. Per accelerare il tutto, è possibile impostare una chiave come default per gli sms mandati a un gruppo di utenti selezionati. Quando il destinatario degli sms è un utente del gruppo, quindi, la chiave di default è usata in automatico e l'utente non deve scriverla ogni volta.

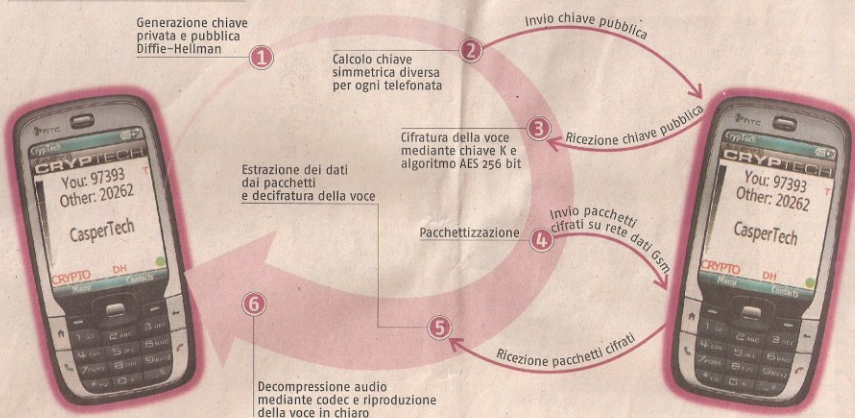
Come fa invece Easy Cryptech a scegliere in automatico la chiave da usare per la chiamata? Tramite l'algoritmo del protocollo Diffie-Hellman. È la prima cosa che fanno due terminali: in automatico si mettono d'accordo sulla chiave. Prima di tutto ne scelgono una che è detta pubblica: anche se viene intercettata non basta per decrittare la chiamata. Ogni terminale separatamente mescola poi la chiave pubblica con una privata, generata internamente. Si ottiene così una terza chiave, che è quella in effetti usata per la comunicazione. Fin qui è usato appunto il Diffie-Hellman, che ricava la terza chiave con un algoritmo di esponenziazione a 4.096 bit.

Parte la conversazione: le parole sono trasformate in pacchetti dati e quindi criptati con la terza chiave con un algoritmo Aes 256 bit. È stato calcolato che per decrittare con un attacco "brute force" (cioè tirando a indovinare), un computer avrebbe bisogno di parecchi anni di tempo (da alcuni a qualche milione, a seconda della sorte). I pacchetti criptati sono poi inviati tramite un canale dati Gsm all'altro terminale, che decodifica la voce e la decrittata. Il tutto avviene in tempo reale, con un ritardo di poco inferiore a un secondo.

Un'eventuale intercettazione (legale o no) non potrebbe così decifrare il contenuto della chiamata. Le autorità, però - spiegano da Caspertech - possono sempre ottenere con un mandato, dall'operatore usato dall'utente, il tabulato della sua chiamata e scoprire così a chi ha telefonato e quando; in certi casi, sapere anche dov'era (tramite geolocalizzazione rilevata dalle celle Gsm). Il solo modo per evitarlo, sarebbe installare un software con cui si modifica il codice identificativo del cellulare, il che però è illegale e comunque sarebbe impossibile sui prodotti Caspertech (l'installazione di altri applicativi è bloccata).

ALESSANDRO LONGO

A prova di intercettazione



PRIVACY TRA TECNOLOGIA E QUESTIONI LEGALI

Sicurezza racchiusa in una chiave

Quanto è sicura la criptazione fatta dai prodotti Caspertech? Com'è possibile che le leggi permettano di usare prodotti davvero a prova di intercettazione? Novaz4 ha rivolto le domande ad alcuni esperti della materia. «Non comprendi mai un criptofonino», dice Miriam Tomponzi, nota investigatrice esperta di tecnologia. «Non posso fidarmi - continua - il punto debole di questi strumenti potrebbe essere che Caspertech fornisca alle autorità una chiave di decrittazione della chiamata. E allora anche un criminale può ottenere la chiave, sfruttando contatti presso qualche pubblico ufficiale corrotto». Caspertech nega che sia possibile: «Da noi non passa niente, non custodiamo le chiavi. È tutto nel software del cellulare, che dopo ogni chiamata distrugge la chiave usata. La volta successiva ne genera una nuova». Se è così, la chiave non può finire in mano a estranei. Il solo modo pensabile per intrufolarsi nelle chiamate altrui potrebbe essere fare un'intercettazio-

Per il momento non è previsto alcun obbligo di pubblicità da parte degli operatori tlc

ne ambientale per sentire quello che almeno uno dei due interlocutori sta dicendo.

Ecco perché si consiglia comunque di usare i criptofonini in ambienti che siano stati appena bonificati da microspie e dove eventuali microfoni direzionali sarebbero visibili (per esempio: in aperta campagna).

«Il tutto è legale e Caspertech non è tenuta a custodire le chiavi. Secondo le nostre leggi, solo gli operatori di telecomunicazioni hanno questo obbligo, per consentire l'intercettazione da parte delle autorità», conferma Andrea Monti,

avvocato esperto di diritto, tecnologia e privacy. «C'è un motivo di fondo: le norme tutelano la crittografia perché resti in piedi il mondo delle transazioni private fatte attraverso telecomunicazioni», continua Monti. Una legge che imponesse alle aziende, fornitrici di servizi di crittografia, di dare le chiavi alle autorità e quindi di custodirle in modo preventivo, renderebbe vulnerabile la sicurezza dell'e-commerce, dell'e-business, delle comunicazioni interbancarie. Sarebbe come far tornare indietro gli orologi dell'economia, sempre più fondata sugli scambi telematici. Oppure, per dirla con Phil Zimmerman, che si difendeva dalle accuse per aver creato quello che ora è il più popolare software di crittografia delle e-mail (Pretty Good Privacy): «Mette fuori legge la crittografia e saranno solo i fuorilegge a usarla». Loro troverebbero comunque un modo per aggirare il problema; il cittadino onesto che ricerca la privacy, no. (a.l.o.)