



## Per cellulari e Voip veramente riservati

Il mondo dei criptofonini, cioè i cellulari che non possono essere intercettati perché muniti di una chiave "segreta" di decrittazione, è vario. In Italia, a produrli è l'azienda torinese CasperTech (nella foto lo smartphone da 1950 euro). Ma esistono anche i codificatori per telefonini. Se collegati ad altrettanti cellulari impediscono qualunque tipo di intercettazione. Ma un nuovo sistema per telefonare senza farsi intercettare viene

anche da Philip Zimmermann, il creatore del sistema di crittazione Pretty good privacy (Pgp), che ha rilasciato una nuova versione di un software pensato per criptare le chiamate effettuate via internet. Zfone, questo il nome del programma, si basa sul protocollo chiamato Zrtp e può essere utilizzato con qualsiasi apparecchio compatibile con lo standard Sip. La prossima settimana «Nova24» pubblica l'intervista a Philip Zimmermann

**CODICI SEGRETI** LA TUTELA È PROTETTA DA UN SOFTWARE

# Contro le intercettazioni c'è il criptofonino

DI ALESSANDRO LONGO

Come proteggersi dalle intercettazioni telefoniche? I modi e le tecniche, certo alla portata del manager, in verità abbondano. Sorprende persino che tanta gente importante sia cascata nella trappola. Per esempio, adesso c'è la moda dei criptofonini. Cellulari che montano software in grado di crittografare con una chiave Aes a 256 bit le chiamate, in tempo reale. Il trucco funziona solo se la comunicazione avviene tra due criptofonini dotati dello stesso software. A produrli in Italia è CasperTech, azienda torinese. Li vende anche in Spagna, Germania, Sud America e Nord Africa.

«Particolarità del nostro prodotto è che evolve di pari passo con l'uscita di nuovi terminali» spiega Ferdinando Peroglio, il direttore commerciale. CasperTech vende due modelli che montano questo software crittografico, uno smartphone da 1.950 euro e un palmare-cellulare da 2.050 euro (più Iva); «se l'utente vuole aggiornare il proprio terminale glielo sostituiamo, con un costo tra i 300 e gli 800 euro, a seconda del modello scelto, più 100 euro di installazione del software», aggiunge. In ogni caso,

*Impossibile anche per le autorità decodificare le chiamate senza avere la chiave*

visti i costi, sono terminali di alto livello, con processore a 200 MHz, 128 Mb di memoria; «presto offriremo anche quelli Umts».

Altri produttori mondiali di criptofonini, invece, usano un hardware fisso, cioè sempre lo stesso terminale per anni. È il caso di Siemens (l'S35 crittografico costa 3.700 euro), Enigma (1.600 euro, ma solo dual band), i russi di Cts (4.000). Funzionano così: il software prima codifica la voce in formato dati, poi la cripta, quindi la invia al destinatario tramite canale dati Gsm (la chiamata costa quanto una normale). Il software ricevente decodifica la voce e poi la decrypta usando una chiave dati che gli interlocutori si sono scambiati.

«Sono gli utenti a gestire le chiavi, noi non le conserviamo» dice Peroglio. CasperTech vende i cripto-

fonini al governo ma anche a privati «purché siano soggetti qualificati, come prevede il nostro protocollo aziendale», precisa Peroglio.

Però può capitare che una persona abbia noie con la legge dopo avere acquistato un criptofonino. A quel punto, come possono intercettarne le chiamate? «Se sono fatte via criptofonino — aggiunge Pavel Ivanov, product manager di CasperTech — le autorità non possono decifrarle senza avere la chiave; anche con i più potenti calcolatori, a oggi, è impossibile. Possono però ottenere il blocco del cellulare, che così non potrà più essere usato».

Ci sono altri modi per proteggersi: con un apparecchio applicato al cellulare (il cosiddetto scrambler o derby; per esempio Snapcell, prodotto in Israele). Disturba eventuali intercettazioni.

«Ci sono anche modi per scoprire se il proprio cellulare è sotto intercettazione — dice Miriam Tomponzi, presidente dell'omonima e storica agenzia d'investigazioni —. Ci sono software che rilevano quando una linea è deviata per essere ascoltata da una terza parte. Se ne accorgono studiando gli sbalzi di frequenza e i rallentamenti che ne conseguono».

2001

**Echelon e la Nsa.** Nel 2001 un rapporto del Parlamento europeo raccomanda l'utilizzo della crittografia per proteggere i cittadini e le aziende dell'Unione da Echelon, un sistema di monitoraggio delle comunicazioni diplomatiche e militari creato durante la guerra fredda dagli Usa con gli altri Paesi anglofoni. Di recente il sistema sembra sia stato utilizzato dalla Nsa per spiare milioni di cittadini americani.

2004

**Intercettati abusivamente.** Il premier di Atene, i capi della Polizia, i vertici delle Forze armate e dell'intelligence, esponenti politici e imprenditori: finiscono nei guai Ericsson e Vodafone, perché nel software delle centrali di telefonia mobile c'è una "pulce". Il 7 marzo 2004 Costas Tsalikidis, dirigente di Vodafone, viene trovato impiccato: si pensa a suicidio, ma è giallo.