PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 385 di venerdì 20 luglio 2001

Echelon: in arrivo un sistema per "difendersi"?

Allo studio di alcuni esperti un progetto per la cifratura dei dati.

Una recente inchiesta europea (cfr. i numeri 149 e 348 del quotidiano) ha dimostrato che Echelon, il sistema di intercettazione planetario americano, esiste e ascolta qualsiasi tipo di comunicazione in forma elettronica: telefonate su rete fissa e mobile, trasmissioni di fax, e-mail e trasmissioni via satellite.
Scopo delle intercettazioni non è tanto lo spionaggio militare, quanto l'individuazione di comunicazioni personali e commerciali, per poi analizzarle accuratamente alla ricerca di parole chiave.

Per tutelare l'anonimato degli utenti, l'unica via di scampo sembrano essere potenti sistemi di cifratura.
Attualmente un gruppo di esperti è impegnato in un progetto denominato "Cryptobox", un'applicazione di instant messaging decentralizzata, che dovrebbe permettere la criptazione di trasmissioni effettuate via Internet, quali email e file sharing.
Questo network di tipo peer-to-peer dovrebbe garantire un grado di sicurezza mai raggiunto prima, poiché agirebbe su due livelli.
Se si invia un messaggio utilizzando il sistema di cifratura PGP, il contenuto è certamente protetto, ma una eventuale "spia" è in grado di individuare l'identità del destinatario.
Con Cryptobox, invece, nessuno sarà in grado di capire chi è il mittente o il destinatario del messaggio, inviato tramite mail o chatline, nè di individuare il momento in cui è avvenuta la comunicazione.
I messaggi cifrati conterranno, infatti, dati fasulli per depistare eventuali sistemi di monitoraggio. Gli utenti inseriranno l'ID utente di identificazione del destinatario, ma il sistema scambierà ogni volta le chiavi di cifratura.

Nikola Bubic, esperto responsabile del progetto e docente presso la Scuola di Information Technology dell'Università di Ottawa, confida che Cryptobox risulti di facile utilizzo per tutti gli utenti e sia abbastanza generale da poter essere esteso a diverse applicazioni.
Il rilascio è atteso entro la fine dell'anno.
