

INVESTIGAȚII: Interlopții și politicienii își criptează convorbirile telefonice

Tehnologie militară americană pusă în slujba celor certați cu legea



Dezvăluirile din ultima vreme făcute pe tema interceptării și ascultării telefoanelor mobile de către serviciile secrete, mai ales de cel al Administrației și Internelor, au determinat apariția pe piața Hi-tech din România a unor oferte de aparatură telefonică menită să facă imposibilă ascultarea de către altcineva a convorbirilor telefonice private. Din păcate, acest gen de aparatură a început să fie folosită în masă mai ales de infractori, care, ca de obicei au grijă să fie cu doi-trei pași înaintea autorităților, mai ales când este vorba despre tehnologia de ultimă oră ce le poate asigura anonimatul afacerilor ilegale.

Un articol de DORU COPOT

În contextul scenariilor actuale, conceptul de „privacy” poate fi uzitat pentru a justifica folosirea aparaturii respective. De asemenea, același concept a devenit paravanul celor care comercializează la vedere atât aparatura telefonică specială concepută pentru a nu fi ascultată, cât și aparatură sofisticată de ascultare a celorlalte tipuri comune de telefoane din gama GSM. Recent, o firmă specializată în comercializarea aparatelor telefonice speciale a început să emită, folosind bloguri și mesaje E-mail direcționate către anumiți clienți, oferte de vânzare a unor aparate telefonice în sistem GSM care au la bază tehnologie de comunicații militare americane. Nu vom pomeni numele acelei firme deoarece nu vrem ca acest material să fie confundat cu unul publicitar.

Acest gen de aparate au la bază sistemul **Cryptech** (brevet de invenție nr.to2003a337), acesta fiind un software de protejare a comunicațiilor GSM, bazat pe o tehnologie militară de codificare de înalt nivel. Sistemul a fost implementat pe un telefon mobil de tip Qtek 8500, fiind ușor de utilizat, datorită unei interfețe extrem de accesibile. **Cryptech** nu necesită procese de instalare speciale sau setări complexe, telefonul mobil fiind livrat la domiciliul clientului cu software-ul instalat direct de către producător. Sistemul transformă vocea în date, o codifică și o trimite în timp real, prin canalul de date GSM, către un alt aparat echipat cu software **Cryptech**, asigurând o codificare „end-to-end”. Criptarea convorbirilor este realizată prin combinarea protocolului Diffie-Hellman cu algoritmul AES 256 (algoritmul folosit de guvernul S.U.A. pentru protejarea documentelor strict secrete). Cheile de codificare sunt simetrice și sunt ușor de configurat chiar de către utilizator, asigurând în felul acesta o protecție totală. (cheia de codificare nu este cunoscută nici măcar de către producătorul aparatului). Stocarea cheilor simetrice de codificare este protejată de o parolă, iar cheile sunt afișate pe ecran doar în format dispersat (hash), eliminându-se astfel riscul citirii lor, în cazul furtului sau pierderii telefonului. Sistemul permite efectuarea convorbirilor codificate și între aparatele care nu folosesc chei simetrice (comune), numai pe baza protocolului Diffie-Hellman. Această tehnologie beneficiază de o soluție audio, care asigură absența totală a ecoului. Deja la nivel național au fost achiziționate câteva mii de asemenea aparate, clienții provenind din rândul funcționarilor publici, oameni politici, polițiști și nu în ultimul rând lumea interlopă, prețul acestor aparate nefiind deloc de neglijat. Un asemenea telefon poate fi achiziționat la un preț pornind de la 700 de euro.