

Name of Publication: Asharq Al Awsat
 Date of Publication: 29/1/2004
 Page(s) in Publication: 12

الأجهزة الأمنية العربية والشركات تهتم بتقنية الاتصالات المشفرة المعتمدة على تقنية المصدر المفتوح الدول المدرجة على قائمة الإرهاب ممنوعة من الحصول على التقنية الجديدة لكي تعزز أمن اتصالاتها وخصوصياتها

ديب، صمام الشيخ

قد تجد من المستهجن أن تلحا شركات كبيرة محترمة إلى لتسبغ الاستخباراتية اللغوية لتسبغ بها على معلومات حساسة عن منافساتها، وخاصة إذا تعلق الأمر بمنافسة ضخمة كدر عليها شركات الملايين من الدولارات. إلا أن هذا الاستهجن وفقاً لتفسير عربي هو أسلوب متبع لدى كثير من الشركات ذات الأسماء الرنانة، حيث تتبع لها تقنية الاتصالات القديمة السبيل للتصمت على المكالمات الهاتفية من نون رقيب أو وقوع في شرك المخابرات التجارية غير القانونية.

الآن أن هذا العصر الذهبي للتصمت أصبح على وشك الانتهاء بفضل تقنية المانيحة متطورة تعتمد على المصنوع المفتوح في الأجهزة الهاتفية الجواله أو الشائبة، وتضمن تشفير الاتصالات الهاتفية بحيث يصبح من المستحيل التحسس على المعلومات الحساسة التي يتم تداولها هاتفياً. ويرى أس شيبب المدير العام لشركة «إي جي تي» الألمانية المتطورة لهذا النظام، أن الحكومات والشركات على السواء في العالم العربي لا تهتم كثيراً بأمن المعلومات لديها، مما يجعلها عرضة لكمز اختراق يمكن تصوره، سواء كان اختراقاً أمنياً أو تجسساً أو تدميراً لمصالح رجال الأعمال وشركاتهم. ومن القمصن التي رواها



شيبب يعرض هاتف الكريبتوفون المشفر خلال معرض انترسيك بدبي هذا الأسبوع (خاص به الشرق الأوسط)

عن منتجها الجديد، خلال معرض «انترسيك» في دبي المخصص للتقنيات والمنتجات الخاصة بأجهزة الأمن والشرطة والطاقي والإتقان والسلامة. وستتولى الشركة الألمانية توزيع الجهاز الجسد، الذي يحمل اسم «كريبتوفون» cryptophone المتلفة. وتشمل السوق الأساسية المستهدفة لتسويق المؤسسات وكبار المسؤولين الذين تتميز الاتصالاتهم بنوع خاص من الضمانات وتتطلب لئراً من التشفير الأمني، مثل الشرطة والقنصت والمسندة والوزارات والبنوك والمؤسسات الصناعية الأخرى ذات المتطلبات الأمنية.

اعتراضها أو اختراقها يمكن من خلالها رصد وإخضاع كل المكالمات الهاتفية التي تجرى داخل أي منشأة. ويشير شيبب إلى أهمية تأمين الاتصالات بقوله «إن اتصالات الهواتف الجواله العادية لا تكون آمنة بصورة كبيرة كما يعتقد الكثير من المستخدمين. فمن الممكن لأي شخص أن يخترق تلك الاتصالات باستخدام معدات يمكن شراؤها بسهولة، وبالتالي يمكن الاستماع إلى المحادثات الهاتفية للطرف الآخر، ويضيف شيبب أن هذه المسألة لا تمثل مشكلة كبيرة لمعظم المستخدمين غير أن الأمر يختلف كلياً بالنسبة للمستخدمين من المؤسسات التجارية وقنصت الأمن، مثل الشرطة التي تحتاج إلى تأمين اتصالاتها ضد محاولات الاختراق. أما عملية التشفير باستخدام البرمجيات التجارية العادية فهي لا تزيد عن كونها أسلوباً لتأخير الاختراق وليس منهجاً. وهناك نظامان قويتان جداً للرميز الحسابي هما «إيه إي إس» بمقاييس 256 بت و«توفيس»، وهو نظام تشفير فريد يعتمد على وجود مفتاح مطور باستخدام نظام التبادل السري «ديفي-هلمان» 4096 بت، ويؤكد شيبب أن الهاتف الجديد ليس مجرد جهاز يحويه صندوق أسود مع بعض المعلومات الفنية الشحيحة كما هو الحال مع منتجات أخرى مطروحة في السوق. ويضيف نحن نعتزم توفير وحديد كل التماسيل حول عمله الداخلي

حتى قبل أن يشتريه المستخدمون، ويعتبر هاتف «كريبتوفون» الذي يبلغ سعره 1600 دولار أميركي أول منتج يستخدم من حقيقة أن أداء وحدة المعالجة المركزية للأجهزة الاستهلاكية المتقلبة مثل الهواتف الجواله والمساعدات الرقمية الشخصية أصبح كافيًا لنظام تشفير صوتي قوي. كذلك فإن قوة التشغيل تجعل من الممكن مواجهة أي نظام مطور لمراقبة الاتصالات. وتخطط الشركة خلال العام الحالي لبيع 3000 جهاز في الإمارات وحدها، و29 ألف جهاز في دول المنطقة، وبخاصة منطقة الخليج العربي. وينظر لتطوير هذه اللقنية لأن الحكومة الإلمانية تحظر بيع هذه الأجهزة للدول المدرجة على قائمة الإرهاب، فيما يجب على الشركة أن تحصل على موافقة الحكومة إذا ارادت بيع الجهاز لحكومة أو شركة ما. ويقول شيبب إن هذا التقدم في التقنيات سيوفر الوسائل لحماية حقوق المؤسسات وكبار الشخصيات في الخصوصية، في وقت أصبحت فيه عقليات التنصت واسعة النطاق وانتهاك الخصوصية تهدد بيضة الأعمال والتجارة والحرمان المدنية ومستقبل المجتمع. يذكر أن الهاكر الشهير فرانك ريجر الذي يعمل الآن رئيساً تنفيذياً للتقنية بشركة GSMK، الشركة المنتجة للهاتف الجديد، هو من قام بتطوير نظام المصدر المفتوح في هذا الجهاز.