



Cerca nel Sito

Cerca

[home](#) > [articoli](#)

La tua Community
Loghi e Suonerie gratis!
 Rubrica, News personalizzate
 » **Entra!**

:: ARTICOLI

- » Editoriale <<
- » Il Punto Settimanale <<
- » **Interviste** <<
- » Dalla Rete <<
- » L'Avvocato Risponde <<
- » A Ruota Libera <<
- » La Striscia di Barga (Vignette) <<
- » Approfondimenti <<
- » Archivio Rubriche <<

Newsletter
Gratis ogni settimana:
 Le notizie dal mondo TLC
 » **Iscriviti!**

:: NOTIZIE

- » Ultimissime **hot!**
- » Notizie recenti (ultimo mese)
- » Canali Tematici
- » Produttori Cellulari: Novitx
- » Le piu' lette
- » Cerca nell'Archivio delle Notizie
- » Ultime dai Gestori Mobile
- » Comunicati Stampa (VPO)
- » Agenda
- » Virus

» **ARTICOLI** (Torna in cima) «

:: WIRELESS

- » Emulatore Wap Browser
- » Risorse
- » Speed Test
- » I siti Wap/Web consigliati
- » UMTS **upd!**
- » 802.11 (Wi-Fi) **upd!**
- » MMS

:: SCHEDE

- » Gestori: Profili tariffari
- » Schede CELLULARI **hot!**
- » Recensioni CELLULARI **hot!**

:: SERVIZI

- » Loghi gratis via WAP **new!**

Intervista a E.Barkan: il GSM non e' sicuro

domenica 7 settembre

Dott.Barkan, innanzitutto complimenti per la sua scoperta! Prima di entrare nei dettagli, puoi presentare ai lettori di Portel.it lo staff di ricercatori che lavora con lei?

Grazie per i complimenti. Il mio nome è Elad Barkan e sono dottorando nel Dipartimento di Informatica diretto dal Professor Eli Biham, al Technion Institute of Technology. Il Professor Biham si occupa di ricerca nel campo della crittografia, in particolare sullo standard di crittografia dei dati (Data Encryption Standard, DES). Nathan Keller è un ricercatore che lavora nel gruppo del professor Biham.

Il nostro lavoro consiste nel ricercare metodi per la crittografia forzando analizzando gli algoritmi e i protocolli esistenti per verificarne la sicurezza. Nel 2002, abbiamo iniziato a fare ricerca sul sistema GSM, scoprendo un problema di sicurezza che avete descritto.

La domanda probabilmente più importante è: ci dobbiamo preoccupare di quanto avete scoperto?

Ottima domanda! Siamo rimasti sorpresi quando abbiamo scoperto la falla nel sistema GSM. Anche uno studente ai primi passi nel campo della crittografia sa cose che non vanno fatte come sono state fatte nel GSM. Ci siamo chiesti come sia possibile che nessuno prima di noi si fosse accorto del problema.

Se la gente dovrebbe preoccuparsi? Noi facciamo ricerca, non possiamo decidere per gli utenti: abbiamo scoperto un problema di sicurezza, avvisando nei mesi scorsi gli organismi che si occupano di GSM. Il problema attualmente non è ancora stato risolto, dunque GSM e GPRS sono ancora potenzialmente insicuri. Nessun problema invece per la terza generazione.

Che cosa avete scoperto esattamente?

Come illustrato nella ricerca "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", le falle di sicurezza che abbiamo scoperto sottoponendo il sistema GSM ad un attacco sono due. Abbiamo ipotizzato diversi scenari possibili, ad esempio il furto di chiamate o la sostituzione di identità (l'utente A chiama o manda SMS facendo uso del numero dell'utente B) e l'ascolto della conversazione (*eavesdrop*).

Quanto è facile violare il sistema? Che conoscenze sono necessarie, a parte nozioni di crittografia?

È facile fare un esempio pratico basato sul furto delle chiamate. Abbiamo simulato un attacco da personal computer: in meno di un secondo, il nostro personal computer aveva tutte le informazioni necessarie a rubare la chiamata.

- » Trova il Profilo Ideale
- » Trova il Cellulare
- » Confronto tra Cellulari
- » Prefissi d'Italia
- » Prefissi Internazionali
- » GSM Network Info
- » Cerca nel Web con Google **hot!**

:: DISCUSSIONI

- » <http://www.mobileforum.it/>
- » Interfaccia NewsGroup Telefonia

:: DIRECTORY

- » Categorie
- » Ricerca
- » Ultimi inserimenti
- » I piú cliccati
- » Consigliati dalla redazione
- » ITINERARI

:: SPECIALI

- » PUBLIC WLAN FORUM 2003
- » CeBIT 2003
- » 3GSM Congress 2003
- » Smau 2002
- » Nokia 7650 **upd!**

:: PORTEL

- » Chi siamo
- » Who's Who
- » Contatti
- » Copyright
- » Disclaimer
- » Siti Partner
- » Per i Webmaster **hot!**



Che hardware avete usato per la vostra ricerca?

Oltre al personal computer e al software, abbiamo usato un ricevitore radio per le frequenze su cui lavora il GSM, alcuni telefoni cellulari piccola cella per la telefonia mobile.

Si può parlare di "pretty good privacy" per il sistema GSM?

Nonostante i nostri risultati, a quanto ne sappiamo le tecnologie alternative al GSM non offrono maggiore sicurezza. Basandomi sui risultati ottenuti, credo che il GSM non possa garantire un alto livello di privacy.

Avete brevettato la vostra scoperta: perché?

Vogliamo permetterne l'utilizzo solo alle Autorità, per scopi legali.

La GSM Association in un comunicato sostiene che la vostra "non ha molta rilevanza. Non sorprende affatto la comunità poiché le implicazioni pratiche sono praticamente nulle". Che pensa?

Non vorrei in questo momento essere al posto della GSM Association si trovano certo in una posizione favorevole. I risultati della ricerca sono in discussione, il documento che abbiamo prodotto è molto di chiunque lavori nel campo della crittografia. Credo comunque che i sistemi 3G il problema sarà risolto.

Cosa cambierà nel sistema GSM dopo la vostra scoperta? In tempo potremo utilizzare un GSM sicuro?

Difficile dire se e quando cambierà qualcosa. Spero però che le società lavorano nel campo dei servizi per la telefonia, ad esempio sui pacchetti via GSM, non facciano affidamento sulla sicurezza del sistema.

Per avere un sistema di telefonia mobile sicuro, probabilmente dovremmo aspettare la diffusione delle reti 3G. La falla del sistema GSM è infatti presente non solo nella rete, ma anche nei cellulari. Anche se il problema venisse corretto sulle reti, è inverosimile che si possa cambiare il sistema in poco tempo, a quasi un miliardo di persone.

Perché le reti 3G sono più sicure?

Il sistema GSM è stato progettato negli anni '80, senza che venissero noti gli algoritmi per la crittografia. Quando Briceno rese noti gli algoritmi, gli esperti decretarono che il sistema era debole. Nelle 3G, l'approccio è stato differente: i problemi di sicurezza sono stati discussi pubblicamente, permettendo ai ricercatori di testare preventivamente gli algoritmi e correggere i problemi. Il risultato è un sistema più sicuro.

Le 3G sono a prova di attacco?

La crittografia è una scienza che si sta ancora sviluppando. Non può essere che in futuro non ci saranno nuovi metodi per la crittografia: al momento le 3G sono sicure, ma come accade per tutti i sistemi, problemi di sicurezza potrebbero essere scoperti in futuro. L'aver discusso in pubblico la sicurezza della tecnologia ha però abbassato di molto questo rischio.

**Intervista a cura della Redazione
[Cavazzini/Levizzani,**

Traduzione a cura di Massimo C

Notizie correlate:

[- Violato il sistema GSM](#)

[Copyright © 2000 - 2003 www.

✚ [Torna alla lista delle **Interviste**](#)

✚ [Torna in **Rubriche**](#)

© Portel.it - Tutti i diritti riservati

Portel.it o Testata Giornalistica registrata al Tribunale di Milano, n° 687 del 30