# מדעני הטכניון: הצלחנו לפרוץ לרשתות GSM

## חברות הסלולר בעולם נדהמו ■ חוקרים מהטכניון הדגימו כיצד ניתן "לפצח" את ההצפנה המשוכללת בה הן משתמשות ■ באורנג' מרגיעים: "לא ידוע לנו על פגיעה באבטחה"

מאת אמיר גילת ואסף זלינגר

**אם יש לכם טלפון סלולרי מרשת אורנג', כדאי שתשקלו לקרוא את השורות הבאות, אפילו אם אינכם מבינים דבר בטכנולוגיה, ומילים כמו תדרי שידור, הצפנה קולית ו־GSM גורמות לכם בדרך כלל לדפדף מיד לעמוד הבא. הסיבה: מתברר שהרשת הסלולרית בה אתם משתמשים פרוצה לחדירות, כך שבאופן עקרוני יכול כל גאון מחשבים משועמם לפרוץ לטלפון שלכם ולהאזין לו.**

חברות הטלפונים הסלולריים השייכות לרשת ה־GSM העולמית (וביניהן אורנג' הישראלית), משקיעות מיליארדי דולרים באבטחת הרשתות שלהן, ומתגאות בכך שלא ניתן לגנוב מהן שיחות או להאזין למאות מיליוני לקוחותיהן.

כעת מתברר שהמציאות אינה כה פשוטה וכי ניתן בהחלט לפרוץ לרשת ה־GSM. מי שגילו את הפרצה, ובכך הדהימו את אנשי תעשיית התקשורת ומדענים מהעולם כולו, הם דווקא אלעד ברקן, פרופ' אלי ביהם ונתן קלר, שלושה חוקרים מהטכניון בחיפה, אשר הציגו את תגליתם בכנס "קריפטו" שנערך בסנטה ברברה שבקליפורניה.

בבסיס הפיתוח עומדת התגלית כי בזמן שטלפון סלולרי מרשת GSM מבצע את השלבים הראשונים של שיחת טלפון, הוא משדר אותות סנכרון מחזוריים אשר מטרתם למנוע שיבושים באיכות הקול. אותות קבועים אלה, כך מסתבר, יכולים לאפשר לגורם המעוניין בכך "לפצח" את ההצפנות המשוכללות שבהן משתמש הטלפון, ולאחר מכן להאזין לשיחה. לדברי החוקרים, מתכנני ה־GSM פשוט התבלבלו בסדר הפעולות: הטלפון היה אמור קודם כל לבצע את הצפנת השיחה, ורק אז להוסיף את אותות הסנכרון המחזוריים, כך שלא יוכלו לשמש ל"פיצוח" ההצפנה. אולם מסיבה כלשהי הטלפונים מוסיפים את אותות הסנכרון לפני שהם מצפינים את המידע, ובכך חושפים את עצמם לחדירה.

מהטכניון נמסר כי עותק המחקר נשלח לרשויות ה־GSM לצורך תיקון הבעיה, והשיטה נרשמה כפטנט אשר יוכל בעתיד לשמש את רשויות החוק. מחברת פרטנר, מפעילת רשת אורנג' בישראל, נמסר כי לחברה "אין כל ידיעה על פגיעה באלגוריתם המשמש להצפנה ברשתות ה־GSM בעולם", וכי "החברה תעביר כל מידע בעניין לאיגוד העולמי של חברות ה־GSM לשם בדיקה ואבחון".