**תקשורת/** חוקרים מהטכניון: הצלחנו לשבור את מערכת ההצפנה של שיחות ברשתות GSM

# שיחות הסלולר נפרצות

**מאת הדר חורש**

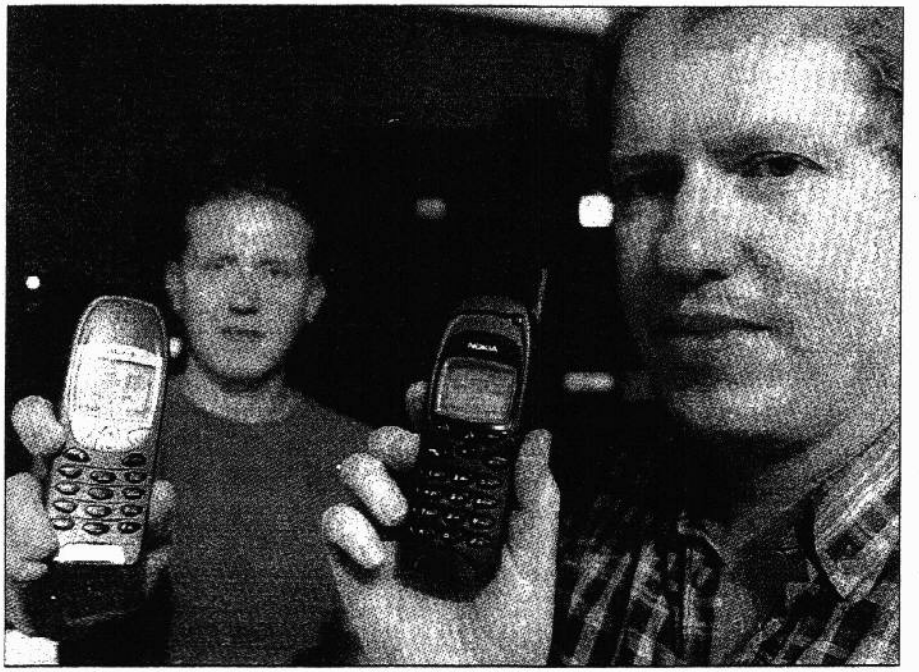
חוקרים מהטכניון בחיפה טוענים כי מצאו דרך יעילה לשבור את מערכת ההצפנה של שיחות ברשתות GSM. צוות החוקרים כלל את פרופ' אלי ביהם, הדוקטורנט אלעד ברקן ונתן קלר. הצוות הציג את ממצאי המחקר בכנס "קריפטו 2003" להצפנה שנערך לפני שבועיים בקליפורניה. הממצאים מעוררים עניין רב בקרב חברות סלולריות ויצרני ציוד, ואולם אף אחת מהחברות אינה מעוניינת עדיין להגיב עליהם.

GSM הוא אחד משני התקנים הנפוצים בעולם לשירות סלולרי. בעולם קיימות כ-540 חברות סלולר המספקות שירותים בתקן GSM, לכ-870 מיליון מנויים. פתרון הבעיה עליה הצביעו החוקרים הישראלים יחייב את החברות הסלולריות, בין היתר, להחליף את כל המכשירים שבידי המנויים, בעוד עד כה נחשבו מערכות ה־GSM לבטוחות יחסית.

המקרה היחיד של האזנות המוניות לטלפונים סלולריים בישראל נודע כ"פרשת ההאזנות" שבה התגלו האזנות סתר לבכירים בעיתונים "ידיעות אחרונות" ו"מעריב". ההאזנות בוצעו באמצעות מערכת שפותחה על ידי חברת ECI ונועדה לשימושם של ארגוני ביון. המערכת היתה מסר גלת ליירט רק שיחות ברשת האנלוגית של פלאפון, והיא אינה יעילה להאזנות לרשתות הדיגיטליות המשרתות היום את מנויי פלאפון, סלקום ופרטנר, שרשת GSM נמנית עמן.

שיטת הפריצה ל־GSM

(סוף בעמוד ג8)



תצלום: אריאל מרגי

ביהם (מימין) וברקן. ייתכן שהחברות ייאלצו להחליף את כל המכשירים שבידי המנויים

# שיחות הסלולר נפרצות

(סוף מעמוד 13)

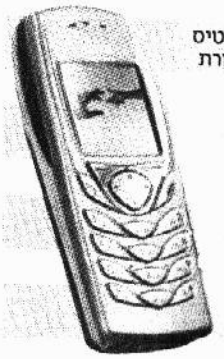
מבוססת על בעייתיות שהתגל־תה בתהליכי הקידוד והפענוח של השיחה הסלולרית; קולו של המשוחח במכשיר סלולרי מתור־גם על ידי המכשיר לסדרה של אותות דיגיטליים, הנושאים את המידע ועוברים תהליך הצפנה המונע ציתות לשיחה. האותות נקלטים על ידי הצד השני, עוב־רים תהליך של פענוח ונהפכים לקול, אותו שומע המאזין.

במשך השיחה נעשה תהליך סינון של האותות העוברים בין המכשיר הסלולרי לאנטנה הסלולרית הסמוכה אליו. בתה־ליך נברר האותות התקינים, בעוד אותות שהצופן שלהם פגום מסיבה כלשהי מסוננים החוצה. תהליך זה מאפשר למא־זין לשיחה לפענח את הקוד של האותות ולהעתיק את נתוני המכשיר המשוחח עם האנטנה.

השיטה שפיתחו החוקרים עשויה לשמש בסיס לפיתוח מכשיר המסוגל לצוד קודים של שיחות, להאזין למשוחחים במכ־שירים שהקודים שלהם נפרצו, ולהיכנס לרשת הסלולרית תוך התחזות לאחד המכשירים עם קודים פרוצים.

לפני כארבע שנים התפרסמו בעולם עבודות של ישראלים, שהצביעו על אפשרות פריצה של קוד ה-GSM. פרופ' ביהם היה אחד החוקרים שמאמריהם פורס־מו, אך הקדים אותו פרסום של פרופ' עדי שמיר, מומחה עולמי לקידוד ומפתח מערכת הקידוד הנפוצה בעולם בתחום הטלוויזיה בלוויין.

## שבירת צופן ה-GSM כך עובדת השיטה



בעת חיוג ממכשיר סלולרי המכשיר "מתקשר" לחברת הסלולר, ומבקש לקיים תקשורת

חברת הסלולר מזהה את הקוד הצרוב בכרטיס ה-sim שבמכשיר ומתחילה בנוהל התקשורת

השיחה מוצפנת באמצעות קוד שנקבע על ידי כרטיס ה-sim

בין המטלפן לחברה מתנהלת תקשורת, במהלכה עוברים אותות שחלקם פגומים

המערכות מסננות את האותות הפגומים ומעבדות את האותות התקינים

המצותת קולט את האותות, ובאמצעות החשוואה בין האותות שהוגדרו פגומים לאותות שנקלטו הוא מפענח את הצופן על פיו פועל המכשיר

בעקבות הגילויים של החוק־רים הישראלים טענו המפעילים הסלולריים כי מדובר ברעיון תיאורטי קשה ליישום, וכי כדי ליישמו על הפורץ לקלוט את השיחה ברגע בו החלה; לטענתם, הסיכוי להצליח במשימה הוא אפסי.

כעת, טוען פרופ' ביהם, מי שישתמש בתוצאות המחקר האחרון יוכל לאתר את קוד המכשירים המעורבים בשיחה באופן מיידי. לדבריו, השיטה מבוססת על שגיאה של מתכנני תקן ה־GSM, שהציבו את תהליך שיפור איכות השיחה לפני תהליך הקידוד. "בחרנו בתקן GSM כי מישהו אחר כבר הוכיח שהתקן המתחרה, CDMA, ניתן לפריצה", אמר אתמול ביהם, "צופן ה־GSM נחשב עד עכשיו לחזק יותר, ועכשיו מצאנו שיטה לשבור אותו. איני עובר עבור חברה מסחרית העשויה להרוויח מהגילוי. אני רק מנסה לבחון את חוזקם של הצפנים".

עד כה לא פורסמה בתקשורת כל שיטה מעשית לשבור את קוד ה־GSM. החוקר הפרטי הוותיק מאיר פלבסקי אמר אתמול כי השיחה הסלולרית נחשבת לבטוחה יחסית וכי אין בשוק האזרחי מכשירים המסוג־לים להאזין לשיחה סלולרית.

עם זאת, המשתמשים בטלפון סלולרי אינם חסינים מפני האז־נות סתר; כל אחד מהמפעילים הסלולריים מצויד במערכת המאפשרת לאתר כל שיחה ברשת שלו ולצותת לה. על פי תנאי הרישיון שקיבלו החברות הסלולריות, הן חייבות לאפשר לרשויות המוסמכות להאזין לכל שיחה, אם הרשות המבקשת מצי־גה צו מתאים מבית המשפט.

ואולם לא כל מי שמבקש להאזין לשיחות סלולריות יכול או רוצה לפנות לבתי המשפט. ארגוני ביון הפועלים במדינות זרות, חוקרים פרטיים ועבריינים היו שמחים להניח יד על מכשיר המאפשר האזנות סתר.

ההנחה המקובלת היא שהסוכ־נות האמריקאית לביטחון לאומי, NSA, פיצחה את הקוד ומסוגלת להאזין לכל טלפון בעולם. לרשותה עומדים תקציבים שגר־לו מאוד מאז 11 בספטמבר 2001. חלק מתקציבי NSA מוע־ברים לארגוני ביטחון של מדי־נות הנחשבות לבעלות בריתה של ארה"ב ומשתתפות במלחמה בארגוני טרור בינלאומיים. הגי־לוי החדש, עליו הספיקו המפת־חים לרשום פטנט, עשוי לאפשר בניית מערכת זולה יחסית לפרי־צת הקוד ולהגביר את הסיכון למשתמשי הטלפונים ברשת GSM.

גם אם חברות הסלולר לא ירצו לסתום את הפירצה שהתג־לתה במערכת האבטחה של תקן ה־GSM, היא צפויה להיסתם מעצמה כשהמפעילים יעברו לדור הבא של התקשורת הסלולרית. לדברי ביהם, הפיר־צה אינה קיימת בתקן "הדור השלישי". ואולם עד שייפרסו מערכות הדור השלישי ויגיעו לכיסו של כל מנוי יעברו כמה שנים. חברת פרטנר מתכוונת לפרוס מערכת דור שלישי בפריסה ניסיונית בשנה הבאה, והפעלה מסחרית של הרשת צפויה רק בסוף 2004 או במשך 2005.