ᎠᏂᏍᏕᏲᏅᏍᏗᏓᏅᏙᏗ

ראש הישראלי עשה זאת שוב: שלושה חוקרים מהטכניון הצליחו לפצח את צופן רשת הטלפונים הסלולריים ״ג׳אס־אם״ – שנחשבת למאובטחת ביותר ● הם גילו את החולשה הסודית ברשת, שמאפשרת לגנוב שיחות, להאזין והתחזות לכל אחד מ־850 מיליון המשתמשים בעולם ● החוקרים מרגיעים: נחשוף את השיטה רק בפני רשויות החוק

מאת **ליאור אל־חי ודודי גולדמן,**
כתבי „ידיעות אחרונות"

שלושת החוקרים הישראלים, שעלו לבמה בכנס „קריפטו" בארה"ב לפני מספר שבועות, החזיקו בידיהם פצצה – והם ידעו את זה. אנשי הפקולטה למדעי המחשב בטכניון הדהימו את 450 משתתפי הכנס, מהמובילים במחקר ההצפנה ובתעשיית ההצפנה בעולם: הם הצליחו לפצח את צופן רשת הטלפונים הסלולריים הפופולרית בעולם.

מה בעצם הצליחו השלושה – פרופ׳ אלי ביהם, הדוקטורנט אלעד ברקן והחוקר נתן קלר – לעשות?

„ג׳י־אס־אם" (קיצור של „מערכת גלובלית לתקשורת ניידת") הוא תקן פופולרי לתקשורת דיגיטלית אלחוטית. מדובר בטכנולוגיה הנפוצה ביותר מבין שלוש הטכנולוגיות הדיגיטליות האלחוטיות. על־פי הערכות, יותר מ־850 מיליון איש – 71% מכלל משתמשי הסלולרי בעולם – משתמשים בתקן הזה.

עד כה, אירגון ה„ג׳י־אס־אם" הצהיר כי טכנולוגיה זו היא המאובטחת ביותר מבין תקני התקשורת הסלולרית. אומנם כבר לפני ארבע שנים הצליחו מספר אנשים לשחזר את האלגוריתמים של הטכנולוגיה, אך הפיצוח נשאר ברמה התיאורטית בלבד. הסיבה? כדי לצותת לשיחה סלולרית היה על המצותת לנחש את תוכן השיחה ברקות הראשונות.

עכשיו – בישראל – הושג הפיצוח האמיתי. „עד עתה לא היו פיצוחים פרקטיים", אומר פרופ׳ ביהם, „המחקר שלנו מראה שקיימת אפשרות לפצח את הצפנים בלי לדעת דבר על תוכן השיחה".

החוקרים הישראלים גילו חולשה יסודית שלא היתה ידועה קודם במערכת ההצפנה של רשת ה„ג׳י־אס־אם", ובאמצעותה הצליחו לפתח התקפה על הצופן. „אנחנו בחנו את החוזק של כל מיני צפנים והגענו לבדוק גם את הצופן הזה. במקור הוא היה סור כמוס ששמרו מפתחי השיטה, ואף אחד לא ידע עליו", מספר פרופ׳ ביהם.

„ברקן, הדוקטורנט, גילה תקלה חמורה במערכת האבטחה של הרשת: הוא מצא כי הרשת עובדת בסדר לא נכון – קודם היא מנפחת את המידע העובר בה, כדי לתקן רעשים, ורק אחר־כך מצפינה אותו. הם עשו טעות, אני לא יודע להסביר אותה. זה איפשר לנו לפתח התקפה חדשה שעובדת בחלקיק שנייה על נתונים שאנחנו שומעים בשידור אלחוטי בלי צורך בשום דבר אחר".

בעקבות זאת פיתחו שלושת חוקרי הטכניון שיטה, המאפשרת לפצח את הצופן כבר בשלב הצילצול, אפילו עוד לפני שהשיחה החלה, ובהמשך להאזין לה. לאחרונה נבחר צופן חדש ומודרני כמענה להתקפות קודמות, אולם חוקרי הטכניון הצליחו להתגבר גם על שיפור זה, כך שלמעשה ההתקפה שתיארו תקפה לכל רשתות ה„ג׳י־אס־אם" בעולם, כולל בארה"ב ובאירופה.

„גילינו שניתן בשיטה הזאת לגנוב שיחות, להקשיב לשיחות, אפילו לחייג בשמך שיחות – כולל במקרים בהם אתה מחייג לבנק ולכל מיני מקומות אחרים והזיהוי שלך הוא על־פי מספר הטלפון", אומר פרופ׳ ביהם. „גילינו בעיה בשיטה וגרמנו שכולם יידעו עליה. כך שיתקנו את הפירצה, כדי שאף אחד לא יוכל להשתמש בזה".

עותק המחקר נשלח לאירגון ה„ג׳י־אס־אם" לצורך תיקון הבעיה, והשיטה נרשמה כפטנט שיוכל בעתיד לשמש את רשויות החוק. החוקרים מבהירים כי לא יפרסמו את תוצאות המחקר ברבים ויחשפו אותו רק בפני רשויות החוק עבור תשלום. על־פי החוקרים, הדרך היחידה לתקן את התקלה היא להחליף את 850 מיליון המכשירים.

איך יושפעו הצרכנים?

אין סיבה לפאניקה

נאמר מייר: אין טעם להיבנס לקרחת של עשייה צרכנית מיותרת ונחפזת, בנוסח החביב כל־כך על הישראלים, שירוצו להחליף את המכשיר. אין במה להחליף.

השיטה הסלולרית של „ג׳י־אס־אם", למרות שפוצחה, היא עדיין בין השיטות הבטוחות ביותר הקיימות בשוק. אפילו המפצחים עצמם רוכשים לשיטה הזו כבור. פשוט צריך להבין שאין שיטה שהיא בטוחה ממעקב במאה אחוז – לא בגלישה באינטרנט, לא בשימוש בשרת־הדואר אצל ספק־האינטרנט, לא בשיחה סלולרית ועקרונית גם לא בשיחה קווית ליעדים ארוכים.

גם לחברות הסלולר אין כמעט מה לעשות, אלא להחליף את כל המכשירים הסלולריים בשיטה הנוכחית – לאחר תיקון, כמובן. צריך להקשיב למומחי הפיצוח, שאומרים שהם מניחים כי הדור הבא של מכשירי הסלולר יהיה כבר חסין נגד חור האבטחה הזה. ואת, כמובן עד שגם בו יתגלו פרצות חדשות. **דודי גולדמן**

החברות בישראל

„החקן מספק את רמת ההגנה הגבוהה ביותר"

בישראל הרשת של „אורנג׳" מבוססת על תקן ה„ג׳י־אס־אם", אותו הצליחו חוקרי הטכניון לפצח, וגם „סלקום" מפעילה רשת בזו.

לחברת „פרטנר" כ־1.95 מיליון מנויי „ג׳י־אס־אם", ואילו לחברת „סלקום", המפעילה שתי טכנולוגיות, כ־600 אלף לקוחות בטכנולוגיית ה„ג׳י־אס־אם".

דובר חברת „פרטנר תקשורת" מסר בתגובה כי תקן ה„ג׳י־אס־אם" מספק ללקוחות הרשת את רמת ההגנה הגבוהה ביותר הידועה ברשת סלולרית. „לחברת 'פרטנר' אין כל ידיעה על פגיעה באלגוריתם המשמש להצפנה ברשתות ה'ג'י־אס־אם' בעולם. פרטנר תעביר את כל המידע בעניין לאיגוד העולמי של חברות ה'ג'י־אס־אם' לשם בדיקה ואימות".

בחברת „סלקום" סירבו אתמול להגיב לידיעה.

יעל גאוני