חוקרי הטכניון: פיצחנו הצופן הסלולרי GSM

החוקרים הודיעו כי הצליחו לפצח את צופן רשת הטלפונים הסלולריים GSM וגילו שאפשר לגנוב שיחות, להאזין ולהתחזות ל-850 מיליון משתמשים ב-197 מדינות.
הטכניון: "נאפשר שימוש בשיטה רק לרשויות החוק"

גל מור

חוקרים מהפקולטה למדעי המחשב בטכניון הצליחו לפצח את צופן רשת הטלפונים הסלולריים הפופולרית בעולם - GSM. הם הציגו את מחקרם בכנס ההצפנה "קריפטו" שנערך בסנטה ברברה, קליפורניה, ועוררו עניין רב בקרב 450 המשתתפים. הפיצוח מאפשר, לכאורה, לצותת לשיחות טלפון של משתמשים סלולריים ברשת ה-GSM, שנחשבה עד כה למאובטחת.

מה זה GSM?

GSM (קיצור של 'מערכת גלובלית לתקשורת ניידת' - Global System for Mobile communication) הוא תקן פופולרי לתקשורת דיגיטלית אלחוטית. מדובר בטכנולוגיה הנפוצה ביותר מבין שלוש הטכנולוגיות הדיגיטליות האלחוטיות: GSM, TDMA ו-CDMA. ה-GSM הופך את שיחות הטלפון שלנו לדיגיטליות, לאחר מכן דוחס אותן ושולח אותן בקשר מוצפן בערוץ תקשורת דו כיווני.

יותר מ-850 מיליון משתמשים ב-197 מדינות משתמשים בתקן GSM, על פי הערכות. בישראל הרשת של אורנג' מבוססת על GSM וגם סלקום מפעילה רשת כזו, במקביל לרשת TDMA. לאור התפוצה הרבה של ה-GSM והסכמי הנדידה (roaming) שחותמים ביניהם מפעילים סלולריים ברחבי העולם, בעלי טלפון סלולרי ברשתות GSM יכולים לקחת עמם את המכשיר למדינות בהן הם מבקרים.

עד כה, איגוד ה-GSM הצהיר כי טכנולוגיה זו היא המאובטחת ביותר מבין תקני התקשורת

אבטחת מידע

GSM. כבר לא כל כך מאובטח צילום:מגזין net

הדפס כתבה
שלח כתבה לחבר

בשיתוף עם PC Magazine ו-netמגזין
>> לחצו כאן להזמנת מנוי

קהילות
פורום מחפשים אתרים
פורום תמיכה

אינדקס
חיפוש אתרים
go

- אינטרנט מהיר
- אחסון קבצים ברשת
- דפדפנים
- אינטרנט
- תרבות דיגיטלית
- פורטלים ומנועי חיפוש
- דואר אלקטרוני (Email)
- מוזר ושנוי במחלוקת
- בניית אתרים

מוצר היום

Net Action
מסך דק שטוח ב - 1399 ש"ח

הסלולרית. אמנם, אמריקני בשם מרק בריצ'נו הכריז על שחזור האלגוריתמים של ה-GSM ופיצוח הצופן עוד בשנת 99', אך הפיצוח נשאר ברמה התיאורטית בלבד בגלל שכדי לצותת לשיחה סלולרית היה על המצותת לנחש את תוכן השיחה בדקות הראשונות. גם פרופ' עדי שמיר, מפתח טכנולוגיית ה-RSA, דיווח בשנת 1999 על פיצוח תיאורטי של אלגוריתמי ההצפנה הסלולרית של תקן התקשורת הסלולרית הדיגיטלית.

מהתיאוריה למעשה

מה חדש בעצם בגילוי של חוקרי הטכניון? "מאז שחזור האלגוריתמים נעשו בעולם ניסיונות רבים לפצח אותם, אך ניסיונות אלו דרשו את ידיעת תוכן השיחה בדקותיה הראשונות כדי לדעת את המשכה", אומר אחד החוקרים, פרופ' אלי ביהם, "מאחר שלא הייתה כל דרך לדעת את תוכן השיחה, לא הגיעו ניסיונות אלה לכלל השלב המעשי. אולם, המחקר שלנו מראה שקיימת אפשרות לפצח את הצפנים בלי לדעת דבר על תוכן השיחה".

ביהם ערך את הדוקטורט שלו אצל פרופ' שמיר, ביחד הם פיצחו בשנת 1991 את הצופן DES ששימש באותו זמן גם את מכשירי הכספומט (ATM) וגילו כיצד ניתן לפצח את הצופן של הכרטיסים החכמים עבור הטלוויזיה דיגיטלית, אשר בבסיס טכנולוגיית ההצפנה של חברת NDS, שהוקמה על ידי שמיר ב-1988.

ביהם, הדוקטורנט אלעד ברקן והחוקר נתן קלר, גילו חולשה יסודית שלא הייתה ידועה קודם במערכת ההצפנה של רשת ה-GSM, ובאמצעותה הצליחו לפתח התקפה על הצופן. "ברקן גילה תקלה חמורה במערכת האבטחה של הרשת", מספר פרופ' ביהם, "בגלל שרשת GSM משדרת בתקשורת דיגיטלית היא מפעילה קודי תיקון שגיאות. הקוד משדר נתונים רבים, כל קוד תיקון שגיאות שולח את המידע כמה פעמים באופן לא מוצפן.

"כל מי שמבין בתחום יודע שקודם מצפינים אחר כך מוסיפים קוד תיקון שגיאות. ב-GSM זה עובד הפוך. לכן, אפשר להשתמש במידע שנשלח בערוץ בלתי מוצפן כדי לגלות לא מעט דברים על השיחה ולפצח את הצופן, גם בלי לדעת את תוכן השיחה. אנשי ה-GSM עשו טעות ואני לא יודע להסביר אותה".

בעקבות הגילוי, פיתחו שלושת חוקרי הטכניון שיטה, המאפשרת לפצח את צפני GSM כבר בשלב הצילצול, אפילו עוד לפני שהשיחה החלה, ובהמשך להאזין לה. בעזרת מתקן מיוחד שיכול גם לשדר, ניתן לגנוב שיחות, ואף להתחזות לבעל המכשיר בעיצומה של שיחה שהוא מנהל. לאחרונה נבחר צופן חדש ומודרני כמענה להתקפות קודמות (עבור דור 2.5), אולם חוקרי הטכניון הצליחו להתגבר גם על שיפור זה, כך שלמעשה ההתקפה שתיארו תקפה לכל רשתות ה-GSM בעולם, כולל בארה"ב ובאירופה.

עותק של המחקר נשלח לאיגוד ה-GSM לצורך תיקון הבעיה, והוגשה בקשה לפטנט על שיטת הפיצוח. החוקרים מבהירים כי לא יפרסמו את תוצאות המחקר ברבים ויחשפו אותו רק בפני רשויות החוק עבור תשלום. על פי החוקרים, הדרך היחידה לתיקון הכשל היא להחליף בהדרגה את 850 מיליון מכשירי ה-GSM ולא ניתן לבצע כל עדכון "מרכזי" לטיפול בבעייה.

(13:35 , 02.09.03)

תגובה לכתבה לדיון בפורום מחפשים אתרים

חזרה לעמוד קודם

אודות האתר | כתבו אלינו | עזרה | מדיניות פרטיות | תנאי שימוש | אתרי הקבוצה
פרסמו אצלנו

Traffic management by radware Site web tracking by NEDSTAT
© כל הזכויות שמורות לידיעות אינטרנט
Site Developed by realcommerce