הטכניון

מגזין הטכניון

סתיו 2003

מפצחי הצופן

עמ' 3

קומבינציה מנצחת:
הפקולטה להנדסת חומרים
עמ' 8-11

כחוט השערה:
קורי עכביש מלאכותיים
עמ' 14

אדריכלות נוף:
לא מה שחשבתם
עמ' 24-26

חוקרי הטכניון הצליחו לפצח את צופן רשת הטלפונים הסלולריים GSM

שלושת החוקרים מבהירים: "רק רשויות החוק יורשו להשתמש במחקר שלנו"

חוקרי הטכניון הצליחו לפצח את צופן רשת הטלפונים הסלולריים הפופולרית בעולם - GSM. הם הציגו את מחקרם בכנס "קריפטו" שנערך בסנטה ברברה, קליפורניה, ועוררו תדהמה ועניין רב בקרב 450 המשתתפים, מהמובילים במחקר ההצפנה ובתעשיית ההצפנה בעולם.

החוקרים - פרופסור אלי ביהם, הדוקטורנט אלעד ברקן ונתן קלר - גילו חולשה יסודית במערכת ההצפנה של הרשת, ובאמצעותה הצליחו לפתח התקפה על הצופן. "אלעד גילה תקלה חמורה במערכת האבטחה של הרשת", מספר פרופסור ביהם. "הוא מצא כי רשת GSM עובדת בסדר לא נכון - קודם היא מנפחת את המידע העובר בה כדי לתקן רעשים, ורק אחר כך מצפינה אותו".

בעקבות זאת 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, אולם חוקרי הטכניון הצליחו להתגבר גם על שיפור זה, כך שלמעשה ההתקפה שתיארו תקפה לכל רשתות ה־GSM בעולם, כולל בארה"ב ובאירופה.

נשיא הטכניון, פרופסור יצחק אפלויג (מימין) עם שר המדע, אליעזר (מודי) זנדברג ומפצחי הצופן - פרופסור אלי ביהם, נתן קלר ואלעד ברקן

ביהם מסביר כי הצפנים נשמרו בסוד, עד שחוקר בשם מארק בריצ'נו הצליח בשנת 1999 לשחזר את האלגוריתמים שלהם. "מאז שיחזור האלגוריתמים נעשו בעולם ניסיונות רבים לפצח אותם, אך ניסיונות אלו דרשו את ידיעת תוכן השיחה בדקותיה הראשונות כדי לפענח את המשכה ואת השיחות שבוצעו אחריה. מאחר שלא הייתה כל דרך לדעת את תוכן השיחה, לא הגיעו נסיונות אלה לכדי מימוש. המחקר שלנו מראה שקיימת אפשרות לפצח את הצפנים בלי לדעת דבר על תוכן השיחה", הוא אומר.

עותק המחקר נשלח לרשויות ה־GSM לצורך תיקון הבעיה, והשיטה נרשמה כפטנט שיוכל בעתיד לשמש את רשויות החוק.

הטכניון יעניק פרסים בסך 100 אלף דולר על רעיונות ופרויקטים בתחום המלחמה בטרור

הטכניון עורך תחרות נושאת פרסים בנושא המאבק בטרור. זאת במטרה לשפר את יכולתן של מדינות העולם החופשי, ומדינת ישראל בפרט, להגן על עצמן מפני גל הטרור העובר על העולם. סך הפרסים ומענקי המחקר - יותר מ־100 אלף דולר. הפרסים נתרמו על ידי ידידי הטכניון בארה"ב, בעקבות מתקפת ה־11 בספטמבר בארה"ב. "נוכח ההתפתחויות המהירות ביכולותיהם של הטרוריסטים נדרשת תגובה יעילה, יצירתית, מתוחכמת ומהירה", אמרו התורמים האמריקנים. "הטרוריזם של תחילת האלף השלישי פולש לחיים הווירטואליים, ועושה שימוש נרחב ומתוחכם בתקשורת האלקטרונית ובאינטרנט הן לצרכיו המבצעיים והן לצרכי תעמולה. הטרוריסטים מהווים קבוצה פנאטית, ערמומית, חשאית ובלתי נראית".

ראש המרכז הטכניוני למדע וטכנולוגיה של בטחון, פרופסור אבי מרמור, אמר כי הטכניון, שהינו המוסד האקדמי הראשון בישראל והמוסד המוביל בתחום הטכנולוגי והמדעי, רואה עצמו מחויב לסייע למדינת ישראל בשעותיה הקשות ולהציע פתרונות יעילים להגנת המדינה ואזרחיה. "התחרות שאותה יקיים הטכניון נועדה לגייס את טובי המוחות לשיפור יכולת ההגנה הישראלית בפני הטרור", הדגיש.

התחרות מתקיימת בשתי קטגוריות נפרדות:

א. פרסים קבוצתיים על הצטיינות בפרויקט שהושלם.

ב. מענקי מחקר לפיתוח רעיונות חדשניים במלחמה בטרור.

בעקבות "קול קורא" שהוציא המרכז למדע וטכנולוגיה של ביטחון, קיבלו ארבעה חוקרים מענקי מחקר מהקרן, ושלוש קבוצות קיבלו פרסים, אשר יחולקו בטקס שייערך בטכניון בתחילת השנה האקדמית הקרובה.