

### לא לעולם חוסן:

#### חוקרים בטכניון הצליחו ליירט תקשורת בלוטות', שנחשבה לערוץ בטוח מפני פריצות

חוקרים בפקולטה למדעי המחשב בטכניון הצליחו לפענח תקשורת בלוטות', שנחשבה לאפיק תקשורת בטוח מפני פריצות. זאת במסגרת עבודת המאסטר של הסטודנט ליאור נוימן בהנחיית פרופ' אלי ביהם, ראש מרכז המחקר לאבטחת סייבר ע"ש הירושי פוג'יווארה בטכניון.

טכנולוגיית הבלוטות', שפותחה בשנות התשעים, הפכה עד מהרה לפלטפורמה פופולרית הודות לפשטות השימוש בה. בניגוד לרשת WiFi היא אינה מבוססת על רשת המקשרת מכשירים רבים זה לזה, אלא על צימוד (Pairing) בין שני מכשירים מסוימים – אוזנייה וטלפון, לדוגמה. שיטה זו מאפשרת שימוש והגדרה נוחים של הצימוד, וגם מקלה על אבטחת התקשורת בין המכשירים.

לדוגמה, כאשר אנחנו מבקשים לדבר בדיבורית בלוטות' עלינו לאשר במכשיר הטלפון את הפעולה. באותו רגע נוצר צימוד בין הדיבורית למכשיר הטלפון. פירוש הדבר הוא היווצרות של ערוץ מוצפן בין שני המכשירים. במשך השנים טכנולוגית בלוטות' התפתחה והתרחבה, והתקדמה לטכנולוגיות הצפנה עדכניות. בשל כך נחשבת טכנולוגיה זו לחסינה מפני התקפות. הודות לפשטותה ולעלותה הנמוכה, נמצאת טכנולוגיה זו כיום כמעט בכל התקן טכנולוגי כדוגמת מכשור לביש, דיבוריות ברכב, טלוויזיות חכמות, שעונים חכמים, מקלדות ומחשבים, ותומכת גם בחיבורי אינטרנט, מדפסות ופקסים.

כעת הצליחו נוימן ופרופ' ביהם, לאחר שנה של עבודה תאורטית וניסויית, לפתח התקפה החושפת פגיעות בתקשורת הבלוטות' על כל גרסאותיה העדכניות. לדברי פרופ' ביהם, מהחוקרים הבולטים בתחום הקריפטוגרפיה כיום, "הטכנולוגיה שפיתחנו מגלה את מפתח ההצפנה המשותף לשני המכשירים ומאפשרת לנו, או למכשיר שלישי, להצטרף לשיחה. כך אנחנו יכולים לצותת לשיחה או לחבל בה. כל עוד לא נשתתף בה באופן פעיל, המשתמש לא יוכל לדעת שיש כאן גורם שלישי שמאזין".

צימוד התקני בלוטות' משתמש ברעיון מתמטי הנקרא בשפה המקצועית ECC – הצפנה בעזרת עקומים אליפטיים. ברגע הצימוד משתמשים התקני הבלוטות' בנקודות על מבנה מתמטי בשם עקום אליפטי באופן שמאפשר להם לקבוע מפתח סודי משותף לשני ההתקנים, שעליו מתבססת ההצפנה בהמשך. חוקרי הטכניון מצאו למעשה נקודה בעלת תכונות מיוחדות הנמצאת מחוץ לעקום, שמאפשרת להם לקבוע את תוצאת החישוב, אך אינה מזוהה כזדונית על ידי המכשיר. באמצעות אותה נקודה הם קובעים למעשה את מפתח ההצפנה, שישמש את שני הרכיבים המצומדים.

המתקפה שפיתחו נוימן ופרופ' ביהם רלוונטית לשני היבטים של בלוטות' – החומרה (צ'יפ) ומערכת ההפעלה (כדוגמת אנדרואיד) בשני ההתקנים המשוחחים (הן באוזניה והן בטלפון במקרה של הדוגמה לעיל) – ולמעשה מאיימת על הגרסאות החדשות ביותר של התקן הבינלאומי. לפיכך הם פנו, באמצעות מרכז תיאום אירועי אבטחת מידע CERT/CC באוניברסיטת קרנגי מלון וארגון Bluetooth SIG לחברות המובילות בתחום ועדכנו אותן בפירצה שגילו. לדברי פרופ' ביהם, "פנינו לחברות ענק ובהן אינטל, גוגל, אפל, קוואלקום וברודקום שמחזיקות ברוב השוק הרלוונטי, וסיפרנו להן על הפירצה ואיך לתקן אותה." ביהם מוסיף "גוגל הגדירו את הפירצה כ"חמורה ביותר" והפיצו עדכון לפני כחודש, וגם אפל הפיצו עדכון השבוע. ובנוסף יצרנים נוספים ששמעו על הפירצה פנו אלינו ביוזמתם לבדיקת מוצריהם."

מידע נוסף מופיע באתר:

<https://www.cs.technion.ac.il/~biham/BT/>

**לפרטים נוספים: דורון שחם, דוברת הטכניון – 050-3109088**