אין מקום

דווקא עכשיו, כשהתחלנו להתרגל לקניות באמצעות כרטיס אשראי באינטרנט, נפרץ קוד ההצפנה בן 512 הביטים. אבל, דונט פאניק, כמו שאומרים המומחים, כי זה לא ממש משחלם לפרוץ כאלה הצפנות ולא לגמרי רלוונטי לאחרי קניות

אורי רבין

uri-ravin@globes.co.il

דווקא בתקופה בה הלקוחות מתחילים לתפוס בטחון, ושהעברת מספר כרטיס האשראי באינטרנט כבר לא נחשבת כהתאבדות פיננסית, בא משת חוקרים בינלאומי והפיל פצצה על עולם הצפנות המידע: צוות ה הצליח לפרוץ מנעול RSA של 512 ביט. להישג זה ישנה חשיבות מיוחדת, בהתחשב בעובדה שמרבית העסקאות באינטרנט מוגנות על ידי הצפנה זו.

אחת הבעיות איתן צריכים להתמודד האחראים על אבטחת המידע היא התפתחותן המואצת של מערכות המיחשוב המהירות, והפיכתן של אלו לשוות לכל נפש. לפני זמן קצר, לדוגמה, הכריזה אפל על מעבד ה-G4 החדש שלה, שמאפשר להכניס הביתה מחשב על של ממש בעלות של אלפי דולרים בודדים. חיבור של כמה מחשבים כאלו באמצעות האינטרנט מעניק לפורצים כוח מיחשוב ששימש בעבר רק ממשלות וגופי מחקר עתירי ממון. וכשמדברים על פריצת הצפנות, לכוח המיחשוב חשיבות עצומה.

גם פרופ' עדי שמיר, אחד מממציאי שיטת ה-RSA, הציג בתחילת מאי מערכת חדשה פרי פיתוחו, אשר מסוגלת להתמודד בקלות יחסית עם פריצת קודים בסדר גודל של 150 ספרות. המערכת, אשר עדיין אינה בנויה, תוכל לשמש לפיצוח ההצפנות של חלק גדול ממערכות תקשורת המחשבים, ובינהן גם תשורות העברת הכספים באינטרנט.

מצד שני, עדיין לא צריך להספיד את שיטות ההצפנה הקיימות. לפי מומחים בתחום הצפנת המידע, גם ההתפתחויות האחרונות עור רחוקות מלאיים על בטיחות המידע - ובכל פעם שהפורצים מתקדמים צעד אחד קדימה, מערכות ההצפנה מתקדמות בשני צעדים.

עסק לא משתלם

ד"ר תמיר טסה, מנהל טכנולוגיות ראשי במחקר אלגוריתמים, חברה המתמחה באבטחת מידע, ישן טוב בלילה גם לאחר פריצת מנעול ה-RSA 512 ביט (ר' מסגרת). לדבריו, שיטות אבטחת המידע וההצפנות הקיימות דורשות מהפורצים השקעה גבוהה ביותר תמורת רווח מזערי, אם בכלל ניתן להרוויח מגניבת כרטיס אשראי מקרי מאתר אינטרנט.

אז מה בעצם קרה?

"מאז '91 מציבה חברת RSA Data Security לפני הקהילה הקריפטוגרפית אתגרי RSA. אתגרים אלו הם מפתחות RSA פומביים, בגדלים שונים, אותם יש לפרק לגורמיהם. המספר שנשבר לפני האחרון היה ה-RSA140, מספר בן 140 ספרות עשרוניות (456 ביט), ובפברואר האחרון הוא פורק לגורמיו לאחר מאמץ חישובי שנמשך קצת יותר מחודש, באמצעות 200 מחשבים אישיים ומחשב על. ב-22 באוגוסט הודיעה קבוצת מומחים בינלאומיים שהצליחה לפצח את RSA155 (155 ספרות, 512 ביט). המאמץ שהושקע היה כביר ונמשך לאורך כ-7 חודשים, אם כי לא ברציפות, והסתמך על 292 מחשבים אישיים ומחשב-על (קריי).

"זהו הישג דרמטי מכיוון שחלק ניכר של פעילות המסחר האלקטרוני באינטרנט מאובטח על ידי RSA עם 512 ביט. אבל אין מקום לפאניקה, משום שאף אחד לא ישקיע כל כך הרבה כסף רק על מנת לשלוף את מספר כרטיס האשראי של אדם כזה או אחר".

אבל מה אם אני מקבל את כל מספרי כרטיסי האשראי של הלקוחות באתר שפרצתי אליו?

"לכל לקוח יש מפתח משלו, ולכן את אותו המאמץ יש להשקיע עבור כל אחד מהמשתמשים. לפיכך אין מקום לפאניקה, אבל בהחלט יש להיות מודעים לסכנות ולתפור פתרון של אבטחת מידע מותאם עבור כל מקרה".

אז ניתן עדיין לסמוך על מפתחות של 512 ביט?

"מפתחות של 512 ביט מספקים בטיחות רבה, אך בהחלט מומלץ להשתמש במפתחות בטוחים יותר. כל הפתרונות שמציעה מחקר אלגוריתמים מסתמכים על מפתחות בני 1,024 ביט. יש להבין ש-RSA בעל מפתח פומבי של 1,024 ביט אינו בטוח 'כפליים' מ-RSA של 512 ביט, אלא הרבה יותר. בטיחות השיטה עולה 'מאד מהר' ככל שגודל המפתח עולה. באפליקציות רגישות במיוחד אנו מציעים מפתחות בני 2,048 ביט".

ולמה לא להשתמש מראש במפתחות באלו?

"כי זה צורך הרבה זכרון וזמן. יש להבין שפעולות הצפנה ופענוח כדוגמת RSA מבוצעות לרוב על גבי כרטיסים וזכמים שיש להם

מה זה "הצפנה"

נושא ההצפנות שעלה לאחרונה לכותרות מעסיק רבים, אבל רק מעטים מבינים באמת מה משמעות המושגים שעומדים מאחורי ראשי התיבות. ד"ר תמיר טסה, מנהל טכנולוגיות ראשי במחקר אלגוריתמים, נותן קצת רקע על העולם אפוף הסוד של המצפינים.

מי מסתח אלגוריתמים להצפנות?

"אלגוריתמים קריפטוגרפיים להצפנות מפותחים בראש ובראשונה באקדמיה, אבל גם במגזרים התעשיתיים והבטחוניים. למשל, אלגוריתם ה-DES הפופולרי פותח בשנות ה-70' על ידי יבמ. אלגוריתם ה-Skipjack פותח על ידי ה-NSA. שיטת RSA פותחה על ידי שלושה אקדמאים - רונלד ריווסט, עדי שמיר וליאונרד אדלמן".

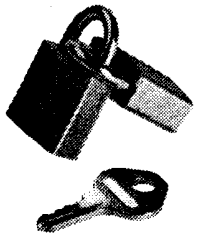
איך, למעשה, מבוצעת הצפנה?

"שיטות הצפנה הן שיטות בהן ניתן להפוך הודעה נתונה, עליה ניתן לחשוב גם כרצף של ביטים או כעל מספר, להודעה אחרת, מוצפנת, כך שקשה מאוד וכמעט בלתי אפשרי לשחזר מתוך ההודעה המוצפנת את ההודעה המקורית. לשם השחזור צריך לדעת מידע סודי נוסף, הקרוי מפתח או מפתח פענוח, שאף הוא מספר או רצף של ביטים. שולח ההודעה בוחר מפתח הצפנה על מנת להצפין את ההודעה, ומפעיל את אלגוריתם ההצפנה על ההודעה הגלויה ומפתח ההצפנה.

"פלט האלגוריתם הוא ההודעה המוצפנת, אותה ניתן לשלוח לצד המקבל. מקבל ההודעה מפעיל את אלגוריתם הפענוח על ההודעה המוצפנת ועל מפתח הפענוח, שאינו שווה בהכרח למפתח ההצפנה, על מנת לשחזר את ההודעה המקורית. מי שמצותת לקו התקשורת, לא יוכל לפענח את ההודעה, גם אם שיטת ההצפנה והפענוח מוכרת לו, מבלי שידע את מפתח הפענוח. לכן, על מנת לשבור את השיטה, יש לגלות את מפתח הפענוח. בטיחותה של השיטה שקולה לעמידותה בפני התקפות המכוונות למציאת מפתח הפענוח".

אלו שיטות הצפנה קיימות?

"קיימות שיטות הצפנה רבות, אבל ניתן לחלקן לשתי קטגוריות: שיטות הצפנה סימטריות ושיטות הצפנה א־סימטריות, הקרויות גם שיטות מפתח פומבי. בשיטות הסימטריות, אותו מפתח שמשמש להצפנת ההודעה, משמש גם לפענוח ההודעה. כך, אם אני רוצה להעביר לך הודעה מוצפנת, נצטרך לפני כן להיפגש בסימטה חשוכה ולהעביר אחד לשני את המפתח, או להסכים על מפתח משותף. השיטה הזו אינה מתאימה כשאני רוצה להעביר מידע לגוף מסחרי דרך האינטרנט, ואין לי אפשרות לתאם את המפתח מראש.



"בשיטות ההצפנה הא־סימטריות, או שיטות מפתח פומבי, קיימים שני מפתחות: מפתח הצפנה (פומבי) ומפתח פענוח (פרטי). משתמש במערכת המבוסס על שיטה א־סימטרית, מפרסם את המפתח הפומבי שלו ושומר אצלו את המפתח הפרטי. כל מי שרוצה להצפין הודעה אליו, ישתמש במפתח הפומבי, ורק אותו המשתמש - שיודע את המפתח הפרטי - יוכל לפענח את ההודעה. כך כל אחד יכול להצפין הודעות עבור אותו משתמש, אבל רק מי שיש לו את המפתח הפרטי - וההנחה היא שזה המשתמש הממוען בלבד - יכול לפענח אותן".

מהי שיטת RSA?

"שיטת הצפנה א־סימטרית, המבוססת על הרעיון הבא: בהינתן מספר גדול מאוד, קשה מאד לחשב את גורמיו הראשוניים. בשיטת RSA המפתח הפומבי הוא מספר ענק המהווה כפולה של שני מספרים ראשוניים. המפתח הפרטי, לעומת זאת, תלוי בשני הגורמים הראשוניים של המפתח הפומבי, כך שעל מנת לשבור את השיטה יש לפרק את המפתח הפומבי לגורמיו וזה דבר שקשה מאד לבצע אותו, ואף בלתי אפשרי אם המפתח מספיק גדול. לפיכך, ככל שהמפתח הפומבי גדול יותר, כך קשה יותר לתקוף את השיטה.

"כשמדברים על RSA של 512 ביט, הכוונה היא שגודלו של המפתח הפומבי, בייצוג בינארי, הוא 512 ביט. גודלי המפתחות המקובלים ביותר הם 512, 768, 1024 ביט".

לדאגה

יכולת אחסון וביצוע רי מוגבלות. אין טעם לפגוע בנחיות המשתמש ולייקר את המוצר, אם המפתח הקטן יותר הוא בטוח מספיק".

מה לגבי אורך החיים של ההצפנות? האם הוא תלוי ומתקצר עם העלייה ביכולת של המחשבים?

"התקדמות ביכולת הקריפטו־אנאליטית לשבירת מפתחות עשויה להגיע משני כיוונים: מהכיוון המתימטי־אלגוריתמי ומכיוון החומרה. התקדמות בכיוון הראשון פירושה פיתוח שיטות מתמטיות יעילות יותר מאלו הקיימות היום. בכיוון זה חלה התקדמות משמעותית מאמצע שנות ה־70 עד שנת 93', ומאז לא חלו שיפורים משמעותיים וסביר להניח שגם השיפורים העתידיים יהיו משניים בחשיבותם.

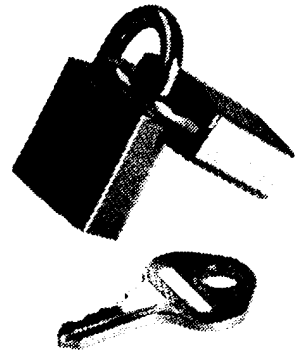
"החומרה, מן הצד השני, הולכת ומשתפרת כל העת, אך אין בקצב שיפור זה - מהיר ככל שיהיה - כדי להוות איום על מפתחות בני 1,024 ביט בעתיד הנראה לעין. אפילו המכשיר התיאורטי שתכנן פרופ' עדי שמיר ממכון וייצמן, ה־Twinkle, שמציע למימוש האלגוריתמים הקיימים חומרה אלקטרו־אופטית המהירה בהרבה מזו הקונבנציונלית, מגדיל רק בכ־100 עד 150 ביט את האיום על מפתחות ה־RSA. כך, מפתחות בני 768 ביט נראים בטוחים מספיק, אבל המלצתנו היא להשתמש במפתחות בני 1,024 ביט לכל הפחות".

שיטות יעילות יותר

גם יצחק פומרנץ, יו"ר ומנהל טכנולוגי באלירו (Aliroo), מסכים כי פריצת מנעולי ההצפנה היא פעולה שהפכה לבלתי משתלמת. "ריווסט, אחד ממפתחי ה־RSA", הוא מצטט, "אמר פעם שאדם פרטי לעולם לא יוציא מעל ל־25 אלף דולר לשבירת סוד של אדם פרטי אחר, חברה לעולם לא תוציא מעל ל־25 מליון דולר לשבירת סוד של חברה אחרת, ומדינה לעולם לא תוציא מעל ל־25 מליארד דולר לשבירת סוד של מדינה יריבה".

לפי רוח זו, מסביר פומרנץ, אנחנו יכולים להסתכל על התפתחות המיחשוב בשנים האחרונות, לראות באיזה קצב פוחת המחיר של מיליון פעולות מיחשוב בשנייה, ולחשב כמה יעלו מליון פעולות מיחשוב בשנייה בעוד חמישים שנה. "אין שום טעם להצפין סוד פרטי במפתח כל כך חזק", הוא אומר, "שגם בכוח המיחשוב הצפוי בעוד חמישים שנה יעלה מעל ל־25 אלף דולר לשבור אותו".

לפי פומרנץ, שבירת הצפנה היא עניין של השקעה נספית ותו לא. בנוסף תיאורטי, הוא אומר, עבור כל מנגנון הצפנה מספר האפשרויות



שצריכים לנסות בשביל לשבור אותו הוא פונקציה של מספר הצירופים האפשריים של המפתח. "הזמן שלוקח לנסות כל אפשרות כזו", מסביר פומרנץ, "הוא פונקציה של כוח החישוב שעומד לשירותך".

בכל מקרה, פומרנץ טוען כי מבחינה פרקטית נסיון לפרוץ הצפנה הוא הדרך הכי פחות רציונלית לגלות מידע סודי. "הרבה יותר פשוט", הוא מפרט, "להתקבל כעובד בחברת הנקיון שמנקה בחברה, לשלם לאחד העובדים או לצאת עם המזכירה של מנהל המחלקה. העלות של הדרכים הללו לא נמדדת בעשרות או במאות אלפי דולר". לדבריו, ההצפנות הנפוצות כבר היום הן מוגזמות בגודלן.

גם בתור מי שמתפרנס מבניית מערכות הצפנה, פומרנץ מודה שהיתרון העיקרי של הצפנת המידע הוא פסיכולוגי. לדבריו, אדם שמצפין את מה שהוא כותב יכול להיות בטוח שיריביו יחפשו את המידע בדרכים אלטרנטיביות, ולא דרך מנגנון ההצפנה. "אני, למשל", הוא מעיד, "בכלל לא חושש להצפין סודות של החברה שלי במפתחות של 40 ביט. אתה מצפין כנגד סקרנות, עצלנים במקום העבודה או כנגד זה שגנבו לך את המחשב הנייד מהאוטו. לאף אחד אין באמת מוטיבציה להשקיע כסף וזמן בשבירה".

למעשה אתה אומר שאף אחד לא מתעסק בפיצוח הצפנות.

"יש שני מקרים יוצאי דופן: אחד הוא המודיעין הממלכתי, שם אנשים מקבלים משכורת כדי לשבור צפנים. אבל תשאל את עצמך כמה שוברי צפנים יש למיקרוסופט, ג'נרל מוטורס, ג'נרל אלקטריק או פוג'יטסו. בלי לבדוק, ברור שהתשובה היא אפס.

"המקום יוצא הדופן השני, שמתקשר למה שקרה לאחרונה, זה בתחום הספורט. שבירת צפנים הפך להיות ספורט. לפני שנתיים וחצי סטודנט בן 16 מברקלי, באמצעות שיתוף כאלף מחשבים באינטרנט שעבדו בזמנם הפנוי במשך 5 חודשים, שבר את ה־DES 56 ביט, והיה לו גם מזל שהוא הגיע למפתח הנכון אחרי 25% מהנסיונות. היו אז שתי צהלות בעולם – היתה צהלה של כל הפריקים ותומכי חופש הביטוי, והיתה צהלה של כל המשתמשים בהצפנה, שאמרו 'נו, אם זה לוקח 5 חודשים לאלף מחשבים והרבה מזל, אז אין דבר בטוח מזה'. אני חושב שמבחינה עסקית עדיף להיות בקבוצה השנייה".

ומה לגבי ההתפתחות המואצת בכוח המיחשוב?

"כיוון שלהגדיל גודל של מפתח זה לא סיבוך גדול, אז במערכות שיתוכננו מכאן ואילך יגדילו את גודל המפתח והספורטאים ידוכאו לעוד כמה שנים. ברוב המערכות הקיימות היום להגדיל ב־2-3 ביטים את המפתח זה אפילו לא שינוי תוכנה, זה שינוי של פרמטר - והגדלה של מפתח בביט אחד מגדילה את זמן השבירה שלו פי שתיים".

לא על ההצפנה לבדה

"כשמדברים על תחומים של הצפנה", אומר ד"ר דני רטנר, קצין אבטחת מידע ב־NDS, "לא תמיד החשוב הוא רווקא הדאגה לחשאיות והפרטיות. למשל, אם מתבצעת קנייה, תרצה להיות בטוח שלא מתחזים בשמך או שלא זייפו את תוכן המידע, או שלא תהיה אפשרות להתכחש למשלוח ההודעה. בנושאים הללו מה שחשוב הוא האימות (Authentication), כלומר, היכולת להוכיח שאתה זה אתה והיכולת לחתום בצורה דיגיטלית. החתימה תאשר שאתה הוא זה ששלח את ההודעה על תוכנה".

לפי רטנר, רמת ההצפנה מותנית בשני גורמים עיקריים: ערך הסוד ומשך הזמן בו צריך שהסוד יישמר. "אם אתה רוצה לקנות מחר אלפיים מניות", הוא מסביר, "ואחרי שתקנה אותן בכל מקרה תודיע שקנית אותן, כל מה שאתה צריך זו הצפנה שתחזיק 24 שעות. מצד שני, אם רכשת את תמונת החמניות של ואן גוך, ואתה רוצה לשים אותה אצלך במחסן בלי שאף אחד יידע, אתה צריך הצפנה שתחזיק כמה עשרות שנים".

גם רטנר, כמו טסה ופומרנץ, אינו מודאג מחסינות ההגנות הקיימות. "צריך להבין שהמצב היום", הוא מסביר, "אם אני מסתכל על הצפנת RSA של 512 ביט, הוא שהיה אירוע אחד בו מאות מחשבים שעבדו 7 חודשים במקביל הצליחו לשבור מקרה בודד של RSA". ובכל מקרה, מסביר רטנר, מעבר ליכולת לפרוץ את מפתח ההצפנה דרושות גם היכולות לדעת מראש היכן בריוק מסתתר המידע הנחשק ומהו המפתח המדוייק אותו יש לפרוץ על מנת להגיע למידע זה.

והמצב הזה לא ישתנה בעתיד?

"בנושא של פריצת הצפנות RSA אין התקדמות דרמטית אלא איטית ולאורך זמן, ולכן מפתחות של 768 או 1,024 ביט צפויים להישאר בטוחים עוד הרבה מאוד שנים - אלא אם תהיה התקדמות משמעותית בפתרון הסיבוכיות של הפירוק של מספרים, ואז בכל מקרה זה יחסל את השיטה. השאלה האם ניתן לפרק מספרים עצומים לגורמים ראשוניים, מעסיקה מתמטיקאים כבר אלפי שנים ועדיין לא נמצאה דרך כזו. ההתקדמות התיאורטית המשמעותית ביותר שהיתה, שגם היא לא מהווה סכנה, הוא התקן ה־Twinkle של פרופ' עדי שמיר".

ומבחינת החומרה הזמינה לנוכלים, מסכם רטנר, זו עדיין רחוקה מלהוות איום משמעותי על ההצפנות המקובלות כיום, כאשר רק לרשויות ממשלתיות יש את כוח החישוב הנדרש לפריצות של הצפנות אלו.