17 בספטמבר 2021

אבטחת מידע 10313

<u>פתרון תרגיל 4</u>

מרצה: ד"ר עמית קליינמן

בודק: ערד פלד

1. פרוטוקול SRP

א. הערך a הוא ערך אקראי שחושב על ידי קרול, והערכים b ו-u נבחרו באקראי על ידי סטיב.

ב. הערך x חושב על ידי קרול מתוך ה-ID שלה, הסיסמה האישית שלה וערך המלח שבחרה. נוסחת החישוב ידועה לכולם, למשל $x = H(P \| ID \| s)$, הערך x לא. x נמסר באופן מאובטח לסטיב בעת רישום המשתמשת קרול. סטיב שומר את הערך x (ע"פ אינדקס ID של קרול). קרול לא שומרת את הערך x.

ג. הערך v חושב ע"פ הנוסחה: $v=g^x$, הן ע"י קרול והן ע"י סטיב. נשמר רק ע"י סטיב.

ד. N הוא מספר ראשוני בטוח (safe prime) וגדול, ידוע לכולם. מספר ראשוני בטוח מציין את עובדת היותו של N ניתן להצגה כ- $N=2p+1$, כאשר גם p הוא ראשוני (למעשה p נקרא sophie germain prime).
למספרים שהם safe prime יש תכונות שמקשות על טכניקות ידועות לחישוב לוגריתם דיסקרטי, שנדרש לפגיעה בפרוטוקול.
H – פונקציית גיבוב קריפטוגרפית ידועה לכולם
g – שורש פרימיטיבי ב- Z_N, ידוע לכולם

ה. סטיב אמור לחשב בעצמו את הערך $H(S_s\|A\|B)$ ולהשוות לערך שקיבל מקרול.

ו. נוסחת החישוב של S_s דורשת לדעת את b, אך ערך זה אינו ידוע לתוקף. הערך היחיד שיש לתוקף שעושה שימוש ב-b הוא B, אך כדי לחלץ ממנו את b הוא נדרש לבצע לוגריתם מודולרי במספרים גדולים, וזו פעולה קשה חישובית.

ז. ההודעה הראשונה בפרוטוקול אינה עושה שימוש בסיסמה.
ההודעה השניה עושה שימוש ב v-שניחוש הסיסמה יכול לגלות אותו, אך גם ב b-שאינו ידוע לתוקף.
ההודעה השלישית עושה שימוש בסיסמה, אך כדי לבדוק איזה סיסמה מתאימה לה התוקף צריך לדעת או את a (אם הוא רוצה לשחזר את החישוב של קרול) או את b (אם הוא רוצה לבצע את החישוב השקול של סטיב).

ח. התוקף יבחר אחת מהסיסמאות, למשל P_1 ויחשב ממנה ערכים x_1 ו-v_1.
התוקף יבחר אחת מהסיסמאות הנותרות, למשל P_2 ויחשב ממנה ערכים x_2 ו-v_2
התוקף ישלח בהודעה השניה בפרוטוקול את הערך v_1+v_2
אחרי שקרול תשלח את ההודעה שלה, התוקף ינסה לבצע אימות, בשתי דרכים שונות:
   i. אם הסיסמה הנכונה היא P_1, האימות יצליח כשבוחרים $v=v_1$, $b=x_2$
   ii. אם הסיסמה הנכונה היא P_2, האימות יצליח כשבוחרים $v=v_2$, $b=x_1$
אם אף אימות לא מצליח, הסיסמה היא האפשרות השלישית, שלא נבדקה.
הערה: חולשה זו הופיעה בגירסה 3 של SRP, ותוקנה בגרסה 6.

ט. לכל תו בסיסמה יש 89=10+27+26+26 אפשרויות.
האנתרופיה:

$$8 * \log_2(89) = 8 * 6.4757 = 51.805867 \approx 51.81$$

2. אליס מבצעת כמה פעולות, ראשית היא מצפינה במפתח הפרטי שלה את גיבוב ההודעה m.
לאחר מכן, היא משרשרת את ההודעה m באופן גלוי ומצפינה את השרשור במפתח הסמטרי.
לבסוף, היא משרשרת את המפתח הסמטרי לאחר שהצפינה אותו במפתח הציבורי של בוב.
בסך הכל, נקבל את ההודעה הבאה – $Ks(PR_A(H(m))||m)||PU_b(K_s)$
מה שבוב יצטרך לבצע הוא תהליך הפוך, ראשית הוא ישתמש במפתח הפרטי שלו כדי לפענח את המפתח הסמטרי אשר משורשר בסוף, בעזרתו הוא יוכל לפענח את השאר.
התוכן שבוב יקבל לאחר פענוח יכיל את ההודעה עצמה ואת החתימה של אליס על ההודעה.
כעת נותר רק לאמת את ההודעה, בוב יגבב את ההודעה הגלויה וישווה אותה עם פענוח החתימה של אליס על ידי פענוח במפתח הציבורי שלה.

3. ההבדל העיקרי בין השניים הוא השימוש במפתח ההצפנה, ביישום Whatsapp, כל הודעה מוצפנת בעזרת מפתחות חדשים וכל עוד הנמען לא ענה, השולח מצרף את המפתחות הציבוריים שלו להודעה.
צירוף המפתחות הינו חלק חשוב מכיוון שהמפתחות החדשים מחושבים בעזרת המפתחות הישנים.
בנוסף, כדי להגביר את האבטחה, ממשיכים לייצר מפתחות ציבוריים ולצרפם להודעות כדי לבצע שינויים נוספים במפתחות ההצפנה.

לעומת זאת, האבטחה בדוא"ל עובדת בדומה לתרשים מהשאלה הקודמת.