16 בספטמבר 2019

אבטחת מידע 10313

<u>פתרון תרגיל 4</u>

מרצה: ד"ר עמית קליינמן

בודק: איתי סוטהלטר

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 26+26+27+10=89 אפשרויות.
האנתרופיה:
$8 * \log_2(89) = 8 * 6.4757 = 51.805867 \approx 51.81$

2. מערכת אימות משתמשים

א. ע"פ פרדוקס יום ההולדת:

$$k = 2^{\frac{n+1}{2}}\sqrt{\ln\frac{1}{1-\gamma}}$$

$\gamma \equiv prob\ for\ at\ least\ 1\ collision$ - הערך אותו אנו מחפשים
$n \equiv \#\ of\ output\ bits$ – מספר הביטים של המלח (=10)
$k \equiv \#of\ inputs$ - מספר המשתמשים (= 128)

$$e^4 = \frac{1}{1-\gamma} \quad <= \quad 4 = \ln\frac{1}{1-\gamma} \quad <= \quad \frac{128}{64} = \sqrt{\ln\frac{1}{1-\gamma}} \quad <= \quad 128 = 2^{\frac{11+1}{2}}\sqrt{\ln\frac{1}{1-\gamma}}$$

$$\gamma = 1 - \frac{1}{e^4} \quad <= \quad 1-\gamma = \frac{1}{e^4} \quad <=$$

הסיכוי הינו: 98.17%

ב. מספר ערכי המלח האפשריים הוא 2^{11}=2048
שני משתמשים שבחרו באותה סיסמה יקבלו אותו ערך מגובב אם ערך המלח שלהם זהה (הסיכוי לערך מגובב זהה עם ערכי מלח שונים הוא אפסי).
הסיכוי לכך הוא $\frac{1}{2048}$

ג. התוקף צריך להצליב כל סיסמה במילון עם כל משתמש, כי לכל אחד יש (ברוב המקרים) ערך מלח אחר.
סה"כ התוקף עושה $12{,}000 \times 128 = 1536 \times 10^3$ בדיקות.
בכל שניה הוא עושה 1000 בדיוק, לכן יזדקק ל- 1536 שניות, שהם 25.6 דקות.

ד. מתקפה מילונית עושה שימוש בערכי המלח שנבחרו בפועל למשתמשים. הגדלת הכמות האפשרית של ערכי המלח לא תשנה את העובדה שלכל משתמש יש ערך מלח משלו, ולכן לא תשפיע על זמן המתקפה.
(הערה: ערך מלח קצר מאוד יכול לגרום לכך שלמשתמשים רבים יש אותו ערך מלח, ולאפשר לייעל מעט את ההתקפה).
מתקפת קשת דורשת לעשות שימוש בכל ערכי המלח האפשריים. כל תוספת של ביט לערך המלח מכפילה את הכמות הזאת, ולכן ערך מלח ארוך הופך את המתקפה ללא אפשרית בזמן סביר.

ה. המערכת הישנה אינה שומרת את הסיסמאות אלא ערך מגובב שלהן. פונקציית הגיבוב היא חד כיוונית, ולכן המערכת לא יכולה לשחזר בעצמה את הסיסמאות המקוריות. החלפת ערך המלח גורמת לשינוי הערך המגובב, ולכן לצורך לחשב אותו מחדש. ללא קבלת הסיסמאות הגלויות מהמשתמשים המערכת אינה יכולה לחשב אותן בעצמה.

3. כלי האבטחה המתאים הינו מלכודת (Honeypot). המלכודת מכילה נתונים ומידי שנראים לכאורה כחלק לגיטימי ממערכות המיחשוב של האירגון ובכך מפתה את התוקף לתקוף דרכה. למעשה מערכת המלכודת מבודדת ממערכות האירגון ומבוקרת. לכן תעבורת התוקף מגיעה אל המלכודת ומשמשת לניתוח והבנת התקיפה (ע"י מערך הגנת המיחשוב של האירגון) אך לא מתאפשרת גישה ותקיפה של מערכות המיחשוב של האירגון.

4. VPN

א. VPN מגן על פרטיות תעבורת מידע העובר על פני רשת ציבורית, כגון רשת האינטרנט. ה VPN מספק מנגנוני אוטנטיקציה, סודיות (ע"י הצפנה/פיענוח) ודאגה לשלמות המידע לנתבים, מגשרים, אתרים, מחשבים ואינדיווידואלים, במיוחד עבור תאגידים ועבור משתמשים ניידים הזקוקים לאבטחת תקשורת מרחוק לרשת התאגידית המקומית.

ב. שני אופני הפעולה של IPSEC הינם:
   i. Transport mode – במוד פעולה זה רק תוכן פקטת ה-IP מאובטח (ע"י אוטנטיקציה ו/או הצפנה). כותרת (header) הפקטת IP נותר ללא שינוי, למעט שדה פרוטוקול ה-IP שמעודכן להיות ESP (50).
   ii. Tunnel mode – זוהי ברירת המחדל לאופן הפעולה של IPSEC. ע"פ אופן פעולה זה כל פקטת ה-IP בשלמותה מאובטחת (ע"י אוטנטיקציה ו/או הצפנה) ועטופה ע"י כותרת (header) וסוגר (Trailer)

ג. ESP וגם AH מספקים הגנה כנגד שידור מחדש של פקטות (replay) המבוססת על מספרים סידוריים. השולח מעלה את המספר הסידורי לאחר כל משלוח של פקטה. המקבל בודק את המספר הסידורי ודוחה פקטה שהגיעה לא ע"פ הסדר.