7 בספטמבר 2019

אבטחת מידע 10313

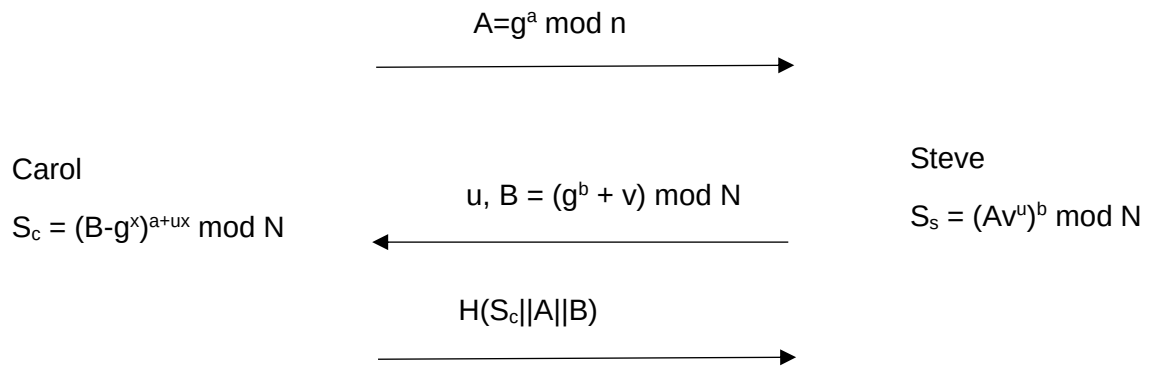
<u>תרגיל 4</u>

יש להגיש לכל היאוחר עד: 16 בספטמבר 2019 בשעה 21:30

מרצה: ד"ר עמית קליינמן

בודק: איתי סוטהלטר

1. התרשים הבא מציג את החלק המרכזי בפרוטוקול SRP לאימות מרחוק על ידי סיסמה בין משתמש (Carol) לשרת אימות (Steve).



א. מהם הערכים a, b ו-u ומי יצר כל אחד מהם?
ב. מהו הערך x? מי חישב אותו? מי שומר אותו?
ג. מהו הערך v? מי חישב אותו? מי שומר אותו?
ד. מהם הערכים g ו-N ו H? מי יודע אותם?
ה. אחרי שסטיב חישב את הערך Ss וקיבל את ההודעה האחרונה מקרול, מה הוא אמור לעשות כדי להשלים את האימות?
ו. נניח שהערך v דלף לתוקף כלשהו, שמנסה להתחזות לקרול ולהשלים את האימות בעצמו. התוקף מתכנן לחשב בעצמו את הערך Ss שמחשב סטיב (במקום Sc), שדורש לדעת רק את v ולא את x. מה יכשיל את תוכניתו של התוקף?
ז. נניח שהתוקף אינו יודע את v, אך הוא משוכנע שקרול בחרה סיסמה קלה לניחוש, שמופיעה ברשימת סיסמאות נפוצות שבידי התוקף. התוקף מתכנן להאזין לתשדורות בין קרול לסטיב בפעם הבאה שיתבצע אימות, ולבדוק איזה מהסיסמאות ברשימה שלו מתאימות לשלושת ההודעות שעוברות בין קרול לסטיב. מה יכשיל את תוכניתו של התוקף?
ח. אחרי פריצה לקובץ אישי של קרול, התוקף הגיע למסקנה שקרול בחרה אחת מבין הסיסמאות הבאות:
   1. את הסיסמה P1=InfoSec.
   2. את הסיסמה P2=1234567.
   3. את הסיסמה P3=MazlTov.

   התוקף מתכנן להתחזות לשרת (סטיב) בפעם הבאה שקרול תבצע אימות מול המערכת, אך לתוקף יש רק ניסיון התחזות אחד. לפי ההודעות שקרול תשלח לו, איך יחליט איזו סיסמה נכונה?
ט. בעקבות נסיונות התקיפה האחרונים על הסיסמה שלה, קרול בחרה סיסמה חדשה. הסיסמה שלה באורך 8 תווים וכוללת אותיות לטיניות גדולות וקטנות, אותיות עבריות (כולל אותיות סופיות) וגם ספרות, אך ללא סימנים נוספים. מהי האנתרופיה של סיסמה כזו? חשבו בדיוק של שתי ספרות אחרי הנקודה.

2. מערכת לאימות משתמשים שומרת פרטים של 128 משתמשים. כל הסיסמאות נשמרות באופן מגובב (hashed) עם ערך מלח (salt) של 11 ביטים.

א. מה הסיכוי שלפחות לשני משתמשים (מתוך 128 המשתמשים הנ"ל) הוקצה אותו ערך מלח? חשבו באחוזים ובדיוק של שתי ספרות אחרי הנקודה.

ב. נניח ששני משתמשים בדיוק בחרו באותה הסיסמה. מה הסיכוי שהערך המגובב שנשמר עבורם יהיה זהה?

ג. נניח שטבלת הסיסמאות (המגובבות) נפלה לידי תוקף. התוקף רוצה לבצע מתקפה מילונית על הקובץ. במילון שלו יש 12,000 סיסמאות. התוקף יכול לחשב את פונקציית הגיבוב 1000 פעמים בשניה. כמה זמן תארך התקיפה? פרטו חישובים

ד. מנהל האבטחה בארגון החליט לשנות את מערכת שמירת פרטי המשתמשים כך שתשתמש בערך מלח ארוך יותר, של 33 ביטים. הוא טוען ששינוי זה כמעט לא ישפיע על הסיכון מפני מתקפה מילונית, אך יגן על המערכת מפני מתקפת קשת (rainbow). הסבירו מדוע הטענה, על שני חלקיה, נכונה.

ה. במהלך הטמעת המערכת החדשה מסעיף ד' (בה שונוה אורך ערך המלח), כל המשתמשים נדרשו לבצע כניסה מחודשת לחשבון שלהם ולספק שוב את הסיסמה שלהם. מדוע לא ניתן להשלים את החלפת המערכת ללא פעולה זו?

3. מנהל האבטחה בארגון רוצה לאסוף תקשורת חשודה שמקורה מחוץ לארגון ומגיעה למחשבים בארגון שלא אמורים לקבל תקשורת כזו, מתוך מטרה להרחיק תוקפים ממערכות מבצעיות וכדי לנתח בזמנו הפנוי את המידע שאסף ולזהות איומים חדשים שלא היה מודע אליהם. על איזה כלי אבטחה עיקרי מבוסס הפתרון שעליו ליישם. הסבר וציין מה מונע מהתוקף לנצל את את (או את התקשורת עם) כלי האבטחה הזה עצמו לביצוע התקיפה.

4. VPN

א. אילו פגיעויות אבטחה מוגנות ע"י VPN?

ב. מהם שני אופני הפעולה של IPSEC? תאר/י כל אחד מהם

ג. מי מהפרוטוקולים AH ו ESP מספק הגנה כנגד התקפת שידור מחדש (replay) וכיצד?