הטכניון - מכון טכנולוגי לישראל

הפקולטה למדעי המחשב | סמסטר אביב תשפ״ב

הגנה ברשתות 236350

תרגיל בית מס׳ 4

הגשה: עד יום ד׳, 01/06/2022, 23:59

הגשה ביחידים

חל איסור חמור על החזקת פתרונות של סטודנטים אחרים. על כל סטודנט לרשום את תשובותיו **עצמאית** ובמילותיו שלו.

נא להגיש את התרגילים אלקטרונית בלבד

בנוגע לשאלה 1 נא לפנות לטל (talneoran@cs)

בנוגע לשאלה 2 נא לפנות לתום (tomazoulay@cs)

בנוגע לשאלה 3 נא לפנות לעידן (idel@cs)

שאלה 1 – RSA/MAC/Signatures

1. נתון כי משתמש A יצר לעצמו מפתח RSA פומבי-פרטי והעביר למשתמש B את המפתח הפומבי שלו באופן בטוח. נסמן את המפתח הפומבי של A ב-(e, n) ואת המפתח הפרטי של A ב-(d, n). תהא H פונקציית תמצות קריפטוגרפית בטוחה עליה הסכימו A ו-B.
למרות שהמרצה המליץ על שימוש בהצפנה היברידית, ובמפתח פומבי שונה להצפנה ולחתימה, החליטו A ו-B להשתמש בשיטות המתוארות במשפטים הבאים. עבור כל אחד מבין המשפטים, ציינו אם הוא נכון או לא נכון, הן מבחינה מתמטית, והן מבחינת בטיחות השיטה. הסבירו בקצרה את תשובותיכם.
   a. כאשר A מעוניין להצפין הודעה M ל-B הוא ישלח ל-B את $C = M^e \bmod n$. B יפענח את ההודעה המוצפנת כך: $C^d \bmod n$.
   b. כאשר B מעוניין להצפין הודעה M ל-A הוא ישלח ל-A את $C = M^e \bmod n$. A יפענח את ההודעה המוצפנת כך: $C^d \bmod n$.
   c. כאשר A מעוניין לחתום על הודעה M אותה הוא שולח ל-B, הוא ישלח ל-B את $M||Sig$, כאשר $Sig = (H(M))^d \bmod n$. B יאמת את החתימה ע״י בדיקה האם מתקיים: $Sig^e \bmod n == M$.
   d. כאשר B מעוניין להצפין הודעה M ל-A הוא ישלח ל-A את $C = (H(M))^e \bmod n$. A יפענח את ההודעה המוצפנת כך: $H^{-1}(C^d \bmod n)$.
   e. כאשר A מעוניין לחתום על הודעה M אותה הוא שולח ל-B, הוא ישלח ל-B את $M||Sig$, כאשר $Sig = (H(M))^d \bmod n$. B יאמת את החתימה ע״י בדיקה האם מתקיים: $Sig^e \bmod n == H(M)$.
   f. כאשר B מעוניין לחתום על הודעה M אותה הוא שולח ל-A, הוא ישלח ל-A את $M||Sig$, כאשר $Sig = (H(M))^e \bmod n$. A יאמת את החתימה ע״י בדיקה האם מתקיים: $Sig^d \bmod n == H(M)$.
   g. כאשר B מעוניין לשלוח ל-A הודעה M שהיא גם חתומה וגם מוצפנת, הוא קודם מצפין על ידי חישוב $C = M^e \bmod n$, ואז מחשב את $Sig = C^d \bmod n$ ושולח ל-A את $C||Sig$. A יאמת את החתימה ע״י בדיקה האם מתקיים $Sig^e \bmod n == C$ ואז יפענח על ידי חישוב $M = C^d \bmod n$.
2. עבור כל אחד מהתרחישים הבאים ציינו איזו מבין המנגנונים (Hash, MAC או חתימה דיגיטלית) הוא המתאים ביותר לשימוש בתרחיש זה. הסבירו את אופן השימוש במנגנון ונמקו בקצרה מדוע הוא המתאים ביותר מבין השלוש.
   a. לאתר שיתוף הקבצים ״שיתוף מהיר״ יש מנהל יחיד, בוב, שמעלה קבצים לאתר ומשתמשים רבים המורידים קבצים. המשתמשים רוצים לוודא שהם מורידים אך ורק קבצים שבוב העלה לאתר. הציעו פתרון המאפשר להם לעשות זאת, כך שאם האתר נפרץ ומישהו אחר העלה אליו קבצים או שינה קבצים קיימים הם יוכלו לזהות זאת ולהימנע משימוש באותם קבצים. ניתן לאחסן באתר מידע נוסף אך צריך להניח שבמקרה של פריצה לאתר הפורצים יכולים לשנות גם אותו.

b. ברשת של חברה מסוימת יש שרת גיבוי קבצים אליו העובדים מעלים קבצים לצורך גיבוי. הציעו דרך פשוטה לבדוק האם קובץ שעובד רוצה להעלות לשרת כבר קיים בשרת בגרסתו האחרונה, ולכן אין צורך להעלות אותו לשרת שוב. על הפתרון להיות יותר יעיל משליחת הקובץ עצמו לשרת.

c. אתר מכירות באינטרנט שבו ספקים מוכרים מוצרים שונים לחנויות נתקל בתופעה שבה לאחר סגירת עסקה, החנות הכחישה כי היא ביצעה אותה וביקשה את כספה חזרה. הציעו פתרון לבעיה זו תוך שימוש באחד המנגנונים.

3. כזכור, בהינתן מפתח RSA פרטי (d, n), חתימת RSA ללא שימוש בפונקציית תמצות מוגדרת כך:

$$Sig(M) = m^d \ mod \ n$$

כמו כן, בכיתה למדנו על חתימה עם פונקציית תמצות המוגדרת כך:

$$Sig(M) = \left(H(m)\right)^d \ mod \ n$$

כאשר H היא פונקציית תמצות בטוחה.

a. תארו שלושה חסרונות בשימוש בחתימת RSA הרגילה לעומת שימוש בחתימה עם פונקציית תמצות.

b. תארו דוגמה פשוטה לשימוש בחתימה דיגיטלית, אשר יש בה צורך להשתמש בחתימה עם פונקציית תמצות. כלומר, שימוש בחתימת RSA רגילה יאפשר התקפה שאינה אפשרית כאשר נעשה שימוש בפונקציית תמצות. הסבירו בקצרה את ההתקפה והראו מדוע היא אינה אפשרית במקרה בו משתמשים בחתימה עם פונקציית תמצות.

עמית וניר לא מצליחים ליישב ויכוח, ולכן פנו לשקד אשר החליט לבצע הגרלה. ההגרלה תתבצע באופן הבא:
כל אחד משני המתמודדים בהגרלה יבחר ביט באקראי (0 או 1) וישלח את הביט לשקד. שקד יחשב XOR של שני הביטים ואם תוצאת ה-XOR היא 0 עמית זוכה. אחרת אם התוצאה היא 1 ניר זוכה.
התגלה שלעמית יש **יכולת לשמוע את ההודעות אותן שולח ניר לשקד וגם לשנות אותן כרצונו**. לניר לעומת זאת אין יכולות כאלו. לכן, שקד מעוניין למצוא דרך שבה יוכלו הצדדים לשלוח אליו את הביט שלהם בצורה בטוחה.
נתון שלכל אחד מעמית וניר יש זוג מפתחות פומבי-פרטי וכל המעורבים בפרוטוקול יודעים את המפתחות הפומביים שלהם. הסימון Sig(P) הוא חתימת RSA ללא פונקציית תמצות על ההודעה P תחת המפתח הפרטי של השולח.
שקד הציע את הפרוטוקול הבא לשליחת הביטים:
כל אחד מהצדדים בוחר מחרוזת M בת 128 ביטים שבה מחצית מהביטים הם '0' ומחצית מהביטים הם '1' ומערבב את הביטים בצורה כלשהי לבחירתו, ובוחר מספר n בין 1 ל-128. הביט ה-n במחרוזת M הוא הביט שבחר הצד. כל אחד מהצדדים שולח לשקד את ההודעה: **Sig(M) ‖ Sig(n)**.
שקד מקבל את ההודעה קודם מעמית ואז מניר. לאחר מכן שקד פותח כל אחת משתי ההודעות כדי לקבל את M ואת n ובודק שב-M יש אכן אותו מספר של אפסים ואחדים. במידה והבדיקה הצליחה שקד לוקח את הביט ה-n במחרוזת M בתור הביט של המתמודד, אחרת הוא מכשיל את הפרוטוקול.
שימו לב שנשלחות רק החתימות ללא ההודעות עצמן. כמו כן, הניחו כי ידוע וברור כיצד להפריד בין שני חלקי ההודעה המשורשרים. הפרוטוקול מורץ פעם אחת בלבד.

עבור כל אחד מהמקרים הבאים ציינו האם עמית יכול לגרום לכך שהוא ינצח בהגרלה. אם כן, תארו את ההתקפה, אחרת הסבירו מדוע לא.

4. ידוע לכם שהביט שבחר עמית הוא '0'. כמו כן, ידוע לכם שהמחרוזת M שבחר ניר היא '010101...01' (כלומר '0' במקומות האי-זוגיים ו-'1' במקומות הזוגיים) ו-n שבחר ניר הוא 26.

5. ידוע לכם שהביט שבחר עמית הוא '1'. כמו כן, ידוע לכם שהמחרוזת M שהגריל ניר היא '000...0111...1' (כלומר '0' במקומות 1-64 ו-'1' במקומות 65-128) ו-n שבחר ניר הוא 5.

שאלה 2 – PKI

חברת Batata העוסקת בייצור מוצרי טכנולוגיה שונים. החברה מייצרת עשרות אלפי מוצרים שונים אשר מיוצרים ונמכרים בעשרות אלפי סניפים שונים ברחבי העולם. כאשר החברה משיקה מוצר טכנולוגי חדש, היא שולחת אותו מהסניף שמייצר את המוצר לכל שאר הסניפים. כאשר המוצר החדש מגיע לסניף היעד, באחריות הסניף לחבר אותו לרשת הסגורה והמאובטחת של החברה על מנת שיוכל להוריד את העדכונים החדשים מהסניף שייצר את המוצר (day-one patch).
בין הסניפים השונים יש תחרות עזה, והם תמיד שמחים לחבל בהשקות מוצר של סניפים מתחרים. על כן החליטו ב-Batata שסניף שיקבל את המוצר יבצע את הורדת העדכונים בצורה מאובטחת על מנת למנוע שינוי זדוני שלהם על ידי סניף אחר (צד שלישי שאינו השולח ואינו המקבל) אשר מעוניין לפגוע בהשקת המוצר.
ניתן להניח כי לכל סניף יש יכולת לבצע MITM על כל סניף אחר.

סטיב, מנהל החברה הציע שעדכוני האבטחה יהיו מוצפנים ב-AES, כאשר בעת השקת מוצר יונפק מפתח סימטרי חדש עבור המוצר. מפתח זה ישלח לכל הסניפים על מדיה נתיקה ביחד עם המשלוח של המוצר עצמו.

1. הסבירו שתי בעיות עם הפתרון המוצע.

כאלטרנטיבה, הציע סטיב שכל סניף ייצור לעצמו זוג מפתחות RSA – $(e,n),(d,n)$. עם המפתח הפרטי הוא יחתום על העדכון, והמפתח הפומבי יועבר באופן גלוי ביחד עם העדכון.

2. האם פתרון זה ימנע פגיעה בעדכונים?

אחראי האבטחה בחברה שמע על תעודות דיגיטליות, ובעצתו הוחלט בחברה להשתמש בהן במקום הפתרונות הקודמים. לכל סניף הונפקה תעודה דיגיטלית על ידי ה-CA של החברה, אשר הוגדר כאמין בכל אחד מהסניפים. כאשר עדכון יופץ, הוא יהיה חתום תחת המפתח הפרטי המתאים למפתח הפומבי שנמצא בתעודה של הסניף. התעודה עצמה תועבר באופן גלוי ביחד עם העדכון.
החתימה מבוצעת על ידי הפעלת SHA256 על ההודעה ואז חתימה בעזרת RSA.

3. נסמן את העדכון ב-M ואת הסניף השולח ב-S. רשמו במדויק מה ההודעה שתשלח, וכיצד המקבל יוודא את החתימה.
4. האם ה-CA חייב להיות נגיש בזמן וידוא תעודה דיגיטלית? הסבירו.

בעקבות הצלחת השימוש בתעודות הדיגיטליות הוחלט להרחיב את השימוש בהן לצרכים נוספים. הוחלט שלכל צורך יהיה CA משלו אשר ינפיק תעודות. זאת אומרת שלצורך הפצת העדכונים יהיה CA משני שייקרא CA_{update}. ה-CA הראשי ששמו יהיה RCA ינפיק תעודה עם יכולת הנפקה ל-CA_{update} ו-CA_{update} ינפיק את התעודות לסניפים השונים לצורך הפצת העדכונים.
בכל סניף יוגדר ה-RCA בלבד כ-CA אמין.

5. רשמו שני יתרונות לשימוש ב-CA משני לצורך הנפקה.

הסעיפים הבאים אינם קשורים לסעיפים הקודמים. אחת השיטות המקובלות בגישה לאתרי אינטרנט היא שהאתר משתמש במנגנון OCSP Stapling בו האתר מקבל מה-CA אישור זמני של OCSP ואותו הוא יכול לשלוח ללקוחות לתקופת זמן קצובה במקום שהם יפנו ל-CA.

6. כיצד שיטה זו עוזרת להגן על פרטיות משתמשים?
7. כיצד שיטה זו מורידה מהעומס הנדרש על השרת?

שאלה 3 – בקרת כניסה

בחברת gitbub החליטו להשתמש בפרוטוקול הבא לצורך הזדהות לקוחות לשרת החברה. לקוחות החברה מבצעים את פרוטוקול האימות הבא:

Client		Server
g^x, ID_c	→	
	←	$\mathbf{g^y, E_{H(pwd_c)}(challenge)}$
challenge	→	

כאשר:

- ID_c הוא מזהה ייחודי של השחקן אשר השרת מכיר.
- g^x ו-g^y - מפתחות Diffie Hellman פומביים, הנבחרים ע"י כל אחד מן הצדדים בכל הפעלה של הפרוטוקול.
- pwd_c - סיסמא אותה תיאם המשתמש באופן מאובטח מול החברה.
- H הינה פונקציית תמצות קריפטוגרפית.
- challenge הינה מחרוזת אקראית שמגריל השרת.
- לאחר סיום הפרוטוקול, ההודעות בין השרת ללקוח נשלחות באופן מוצפן תחת מפתח DH המשותף.
- ההצפנות מבוצעות בצופן סימטרי באופן תפעול מאובטח.

עבור תוקף בעל יכולת MITM:

1. האם הפרוטוקול מוגן מחטיפת הקשר? הסבירו.
2. האם הפרוטוקול מוגן מפני התחזות לשרת? הסבירו.
3. האם הפרוטוקול מוגן מפני מתקפת MITM? הסבירו.
4. האם הפרוטוקול מוגן מהתקפת מילון לא מקוונת (כולל התקפה היברידית)? הסבירו.
5. האם הפרוטוקול מקיים את תכונת ה-PFS? הסבירו.

על מנת להתמודד עם הבעיות הקודמות, החברה הציעה לשנות את הפרוטוקול באופן הבא:

$\mathbf{ID_c, E_{H(pwd_c)}(g^x)}$	→	
	←	$\mathbf{E_{H(pwd_c)}(g^y), E_K(g^x, challenge)}$
$E_K(\text{challenge})$	→	

- K הינו מפתח ה-DH המשותף.
- לאחר סיום הפרוטוקול, ההודעות בין השרת ללקוח נשלחות ללקוח באופן מוצפן.
- שאר הערכים זהים לפרוטוקול הישן.

עבור תוקף בעל יכולת MITM:

6. כיצד הלקוח מאמת את זהות השרת? כיצד זה מונע התחזות לשרת?
7. כיצד השרת מאמת את זהות הלקוח? כיצד זה מונע התחזות ללקוח?
8. כיצד הפרוטוקול מונע MITM? הסבירו.
9. כיצד הפרוטוקול מגן מפני מתקפת מילון? הסבירו.