שם המגיש: עומר גרייף

ת"ז : 2082000154

תאריך הגשה: 16/06/23

שאלה 1 – PKI :

1. OCSP -> פרוטוקול זה נועד לבדוק האם סרטיפיקט ספציפי כלשהו בוטל על ידי הCA . בפרוטוקול זה המשתמש פונה אל הCA ומבקש ממנו בדיקה ספציפית האם הסרטיפיקט בוטל. הCA מחזיר תשובה לגבי הסרטיפיקט הספציפי בלבד. לכן, פרוטוקול זה מצריך זמינות תמידית של הCA בכל פעם שנרצה לבדוק האם הסרטיפיקט בוטל מכיוון שאנחנו לא מקבלים רשימה עדכנית של כל הסרטיפיקטים.
2. CRL -> רשימת סרטיפיקטים מבוטלים עבור CA מסוים. המשתמש צריך אחת לכמה זמן לפי הזמן שמועדכן אצל הCA כ"זמן הבא לעדכון" או לפי רצון המשתמש את רשימת הסרטיפיקטים המבוטלים אצל הCA . בגישה זו המשתמש לא צריך לפנות לCA על כל בדיקה של CA מבוטל מכיוון שהוא מקבל רשימה כוללת ואם הוא דואג לעדכן אותה בזמן סביר אז הוא יכול לאמת שהסרטיפיקט לא מבוטל מהרשימה שכבר נמצאת אצלו. על כן פחות חשובה זמינות של הCA בכל בדיקה של אי ביטול סרטיפיקט.
3. קבלת X(365-I) מוכיחה שהסרטיפיקט עדיין בתוקף -> מכיוון שפונקציית התמצות שלנו היא קשה להיפוך, בהינתן X(J) כלשהו ניתן לשחזר את כל הX(I) החל מX(365-J) עד הX(365) על ידי הפעלת תמצות J פעמים ולאחר מכאן לבצע השווה לX(365) לצורך אימות. לעומת זאת לא ניתן לדעת דבר על שאר הX עד J (נובע מאי הפיכות פונקציות התמצות) . על כן שליחת X(365-J) מסוים ביום J תאפשר לכל מי שיקבל את ההודעה להבין כי הסרטיפיקט עדיין בתוקף שכן הוא יוכל לחשב מהX הנתון את X(365) וזהו דבר ייחודי לכל יום ולכל סרטיפיקט מבחירת X(0) אקראי ורק הCA יודע את ערך הX המתאים לכל יום.
4. משיקולים דומים לסעיף הקודם הCA הוא היחיד שיודע את Y(0) לפני החלטה על ביטול ועל כן על ידי הפעלת תמצות על ערך זה הלקוח יכול להפעיל תמצות ולבדוק האם הערך אכן שווה לY(1) וכך לזהות את הסרטיפיקט ברשימת הסרטיפיקטים המבוטלים. וכמובן שרק הCA יודע את הערך המתאים שכן הוא הוגרל על ידו ברנדומליות והופעל עליו תמצות ועל כן רק הוא יוכל להכניס את הערך המתאים לסרטיפיקט המבוטל. כלומר אם מצאנו את הY שמתאים לY שלנו אחרי הפעלת תמצות נוכל לדעת בוודאות שהCA הוא זה שהכניס אותו ולא גורם אחר.
5. כפי שציינתי בסעיפים הקודמים מדובר במשימה קשה ועל כן לא אפשרית שכן בהסתכלות של שנה כאשר הI לא חוזרים על עצמם, ידיעת הX של היום הנוכחי וכל ה-X של העבר לא יעזרו לפענח את היום הבא שכן ניתן להניח שפונקציית התמצות חזקה דיו.
6. עבור מקרה זה לא יהיה ניתן להחזיר את הסרטיפיקט להיות מאושר מכיוון שלאחר ביטול הסרטיפיקט הCA דואג לנקות את כל הX הרלוונטיים לסרטיפיקט מהטבלה אצלו. לכן, בהינתן הקושי להפיכת התמצות כפי שתואר עד כה לא יהיה ניתן לשחזר את הXים שהCA נדרש להמשיך לשלוח ללקוח כדי לאפשר המשך אימות של הCA.

7. ראשית על מנת להבחין בין Y(0) לX(365-i) ניתן לבצע הבחנה ראשונית לפי אורך הקלט. אם הוא באורך 160 ביט נדע שמדובר בY(0) אחרת X(365-i) . וכמובן שלאחר מכאן נדרש לבדוק אימות של הערכים כלומר, אם אורך הקלט הוא 160 נפעיל תמצות פעם אחת ונשווה לY(1). קיבלנו אותו ערך -> יש אימות והסרטיפיקט מבוטל. אחרת קיבלנו קלט שגוי. אם אורך הקלט 80 אז נפעיל i פעמים (כמספר הימים שחלפו) פונקציית תמצות ונבדוק האם שווה לX(365) אם כן -> יש אימות והסרטיפיקט קביל. אחרת הקלט שגוי.
8. מכיוון שבשיטה החדשה לא נשלחת רשימה אלא נשלחת בקשה של המשתמש אל הCA לבדיקת ביטול, אנו נדרשים להבחין בקלט האם מדובר בY או X. לכן אם למשל המשתמש יסתפק בבדיקת אורך הקלט על מנת להחליט האם מדובר בY או בX , נוכל להעביר קלט באורך X ועל כן המותקף יבחין כי הוא לא קיבל קלט אפשרי ל Y(0) אזי הוא קיבל קלט לX(365-i) ועל כן הסרטיפיקט לא מבוטל לכאורה. לכן לא ניתן להסתפק בכך ועל המשתמש לבצע את כל הבדיקות ואכן לאמת את X(365-i) ולוודא שלאחר הפעלת התמצות מתקבל X(365).

שאלה 2 – Entrance Control

1. **מוגנות מפני חטיפת הקשר:**

הפרוטוקול המוצע מוגן מפני חטיפת הקשר מכיוון שלכל צד בהתקשרות יש מפתח פומבי כחלק מפרוטוקול DH שנוצר באמצעות מפתח פרטי סודי. בעת יצירת ההתקשרות מועבר המפתח הציבורי (ולא הפרטי) מועבר ועל ידי מפתחות אלו כפי שראינו בתרגול/הרצאה ניתן ליצור מפתח ייחודי להתקשרות שרק הצדדים שמחזיקים במפתחות הפרטיים הרלוונטיים יכולים לתקשר אחד עם השני. ומכיוון שלאחר התקשרות ראשונית כל התקשורת מבוצעת על ידי הפצנה מבוססת המפתח המשותף לא תתכן חטיפת הקשר.

2. **מוגנות מפני התחזות לשרת:**

הפרוטוקול לא מוגן מפני התחזות לשרת שכן במהלך תהליך ההתחברות התוקף יכול לתפוס את ההודעה שהשרת מעביר ללקוח עם המפתח הציבורי שלו משורשר עם תמצות האתגר ולשנות בהודעה המועברת את המפתח הציבורי של השרת למפתח של התוקף להעביר זאת ללקוח. ניתן לבצע זאת מכיוון שהמפתח הציבורי לא עובר תמצות שמבוסס על סיסמת הלקוח ולכן ניתן בקלות יחסית להחליף את במפתח הציבורי בהודעה מהשרת למפתח ציבורי של התוקף (כמובן שצריך לקוות שההודעה שלנו תגיע ללקוח לפני ההודעה האמיתית של השרת).
לאחר מכן הלקוח יחזיר את הchallenge ויחשוב שהתוקף זה השרת האמיתי מכיוון שהמפתח המשותף שנוצר מתאים לתוקף וללקוח.

3. **מוגנות מפני MITM :**

הפרוטוקול לא מוגן מפני MITM מפני שבדומה לסעיף הקודם במהלך ההתקשרות ניתן התוקף יכול לקבל את ההודעת ההתקשרות הראשונית בין הלקוח לתוקף ולשמור את המפתח הפומבי של הלקוח. כעת הוא יכול להעביר את שאר ההודעה בשרשור מפתח ציבורי חדש שלו לשרת. השרת יעביר את הchallenge מתומצת בשרשור המפתח הפומבי שלו וגם כאן התוקף יקבל את ההודעה, ישמור את המפתח הציבורי של השרת ויעביר את ההודעה ובה יחליף את המפתח המשורשר להיות המפתח הפומבי שלו ללקוח. הלקוח יחזיר

את הchallenge לתוקף, התוקף יעביר לשרת וכך קיבלנו MITM כאשר ישנו מפתח ייחודי ללוקח-תוקף ולתוקף-שרת מבוסס DH.

4. **מוגנות מפני התקפת מילון:**

הפרוטוקול אינו מוגן מפני מתקפת מילון. מכיוון שהchallenge המוחזר אינו עובר הצפנה, בעזרת challenge ותוצאת ההצפנה של הchallenge מבוססת הסיסמה של משתמש מסוים ניתן להריץ מילון של סיסמאות ידועות על ההצפנה המתאימה לסיסמה שנבחרה מהמילון על הchallenge ולבדוק שווין עם הערך המתאים שנשלח מהשרת בתחילת ההתקשרות. אם נקבל התאמה נדע בסבירות גבוהה שהסיסמה שהזו היא הסיסמא המתאימה למשתמש ונוכל להשתמש בה להתקשרות בסשן חדש מול השרת תחת הזיהוי של המשתמש שקיבל את האתגר המוצפן.

5. **קיום PFS:**

הפרוטוקול מקיים את עקרון PFS מכיוון שכחלק מהפרוטוקול מתבצע שימוש בDH שמגריל עבור כל סשן של התקשרות מספרים אקראיים (מפתחות פרטיים) מהם נגזרים המפתחות הציבוריים של הלקוח והשרת ומהם גם נוצר מפתח אימות משותף לכל תהליך ההתקשרות.

6. **זיהוי השרת על ידי הלקוח:**

כעת מכיוון שאנחנו מצפינים את המפתח הציבורי של הלקוח תחת תמצות הסיסמה רק מי שמחזיק את הסיסמה (קרי השרת אף על פי שזה לא מוחלט) יוכל לפענח את המפתח הציבורי של הלקוח שמהווה חלק במפתח המשותף שייווצר בהמשך לשרת וללקוח לאחר אימות האתגר. בנוסף תהליך זה מונע את ההתחזות לשרת מכיוון שכעת רק בידיעת הסיסמה ניתן לזהות את המפתחות הציבוריים של השרת והלקוח וגם בידיעתם האתגר שמועבר עובר הצפנה מבוססת מפתח משותף של השרת לקוח.

7. **זיהוי השרת על ידי הלקוח:**

השרת מאמת את זהות הלקוח על ידי פתירת הchallenge שמועבר תחת הצפנה מבוססת DH של המפתחות הציבוריים של השרת והלקוח והעברת מפתחות DH תחת הצפנה מבוססת סיסמת הלקוח. השרת מעביר את המפתח הציבורי שלו תחת הצפנה מבוססת הסיסמה הפרטית של הלקוח כך שרק מי שיודע את הסיסמא הפרטית של הלקוח יוכל להשתמש במפתח הפומבי להמשך התקשורת. בנוסף ליצירת מפתח DH כעת האתגר מועבר מוצפן וגם התשובה שהלקוח מחזיר, מוחזרת מוצפנת מבוססת מפתח DH. כל אלו מונעים התחזות של תוקף ללקוח שכן הוא נדרש לדעת סיסמה פרטית כדי להבין את המפתחות הפומביים שעליהם מבוססת התקשורת וגם כדי להבין את האתגר הוא צריך לדעת את הסיסמה. כלומר קשרנו את כל המרכיבים יחדיו וללא ידעת כולם לא ניתן להתחזות .

8. **מוגנות מפני MITM**

הפרוטוקול כעת מוגן מפני MITM מכיוון שמפתחות DH הנתונים מוצפנים תחת סיסמאת המשתמש. לכן בין אם בתהליך ההתחברות התוקף יצליח להאזין לתקשורת, כל ההודעות שמועברות מוצפנות תחת הסיסמא של המשתמש או המפתח המשותף של השרת עם

הלקוח. וכפי שציינו בסעיפים האחרונים לא ניתן להתחזות ללקוח ולכן התוקף לא יוכל לשנות פרטים באמצע ההתקשרות כדי שהם יעברו דרכו.

9. **מוגנות מפני התקפת מילון**

הפרוטוקול כעת מוגן מפני התקפת מילון מכיוון שכפי שצויין בסעיפים הקודמים כל ההודעות שרצות בין השרת ללקוח בתהליך ההתקשרות מוצפנות תחת K או תחת הסיסמה ומכילות באופן הפוך מידע על האתגר או על המפתח. לכן התקפת מילון לא תעזור במקרה זה מכיוון שבכל התקשרות נבחרים מפתחות פומביים חדשים שהם מוצפנים על ידי הסיסמה הייחודית של הלקוח ועל כן יצירת מילון עבורם, עבור כל סיסמה אפשרית היא קשה ועל כן לא תתיכן.

שאלה 3 – RSA

1. **האם נוצר מעגל אמון בין הסרטיפיקטים:**

מאופן בניית מפתחות נRSA והצפנת הסרטיפיקטים לא נוצר מעגל אמון, זאת מכיוון שאם נסתכל למשל על הסרטיפיקט של אליס. ראשית נזכיר שהסרטיפיקט שאליס מחזיקה חתום על ידי המפתח הפומבי לחתימה של בוב כך שרק בוב בעזרת המפתח הפרטי לחתימה שלו יכול לאמת את הסרטיפיקט. בנוסף כאשר אליס שולחת את הסרטיפיקט החתום היא חותמת עליו עם החתימה הפרטית שלה להצפנה כך שרק בעזרת המפתח הפומבי להצפנה שלה שנמצא אצל בוב הוא יכול לפענח את הסרטיפיקט ולאחר מכאן לאמת את נכונותו עם המפתח הפרטי שלו לחתימה.
כלומר כפי שהוסבר פה, לא נוצר מעגל אמון וכל צד יכול להגיע לאימות של הצד השני.

2. **פרימיטיביים סימטריים מול מפתחות פומביים:**
ראשית שתי השיטות ראויות להיות אופציות למנגנון החתימה שכן לשתיהן יש יתרונות וחסרונות ושתיהן מאפשרות אימות של שני הצדדים. השיטה של פרימיטיביים סימטריים אפשרית ואולי עדיפה מכיוון שניתן להגדיר "ברגע הקוסמי" בספריה על המפתחות הסימטריים ולאחר מכן להשתמש בהם באופן ישיר לתקשורת ביניהם. היתרון המשמעותי עבורם הוא שהחישוב והשימוש בהם פשוט ומהיר ביחס למפתחות פומביים (מפתח אחד ישיר לכל פעולת התקשורת). עם זאת כאשר מתגלה המפתח אין ברירה אלה להגיע "לרגע קוסמי" נוסף בו יאלצו להסכים על מפתח חדש.

כעת נתון כי הסגל יודע את המפתחות הפומביים של אליס ובוב.

נעזר בזהות XOR של A = B XOR B XOR A ונזכיר שדף הנוסחאות החדש הוא M'' אותו אנו מחפשים.

3. **האם ניתן לקבל את M'' :**
אם נפעיל את המפתחות הפומביים של אליס ובוב על החתימות של M' ו-M'' נוכל לקבל את M' ו-M'' באופן ישיר. כלומר:

$$if\ given\ sigB(M'')\ than\ we\ can\ do\ \left(sigB(M'')\right)^e =$$
$$> \left(M''^d modn\right)^e modn \qquad => M''\ modn$$

כלומר ניתן לגלות את M'' (n גדול מספיק מנתוני המימדים של דפי הנוסחאות ומפתחות ההצפנה). באופן זהה ניתן לבצע עבור M' אך אין צורך על מנת למצוא את הנוסח הסופי .

4. **<u>האם ניתן לקבל את "M :</u>**

באופן דומה לסעיף 3 אם נפעיל את המפתח הפומבי על החתימה של ההודעה השניה נקבל את $M' \; XOR \; M'' \; XOR \; K$. כעת נבצע *XOR* לביטוי הנל עם החלק הראשון של ההודעה הראשונה המשורשרת $M' \; XOR \; K$, מתכונות *XOR* נקבל בישירות את *M''* וסימנו.
(באופן דומה ניתן להשתמש בביטוי $M' \; XOR \; M''XOR \; K$ ומהחלק הראשון של ההודעה השניה $M'' \; XOR \; K$ נבצע *XOR* עם הביטוי שקיבלנו ונקבל בישירות את *M'*).

5. **<u>האם ניתן לקבל את "M :</u>**

בסעיף זה לא ניתן להפיק את 'M או "M . ראשית נבחין שגם אם נפענח את ההודעות המועברות נקבל את $M' \; XOR \; K$ ואת $M'' \; XOR \; K$ שאלו הן בדיוק החלק הראשון בכל הודעה מועברת ועל כן לא נותנות לנו מידע נוסף. משילוב ההודעות הנל לא ניתן לבודד את אף אחת מהM מכיוון שK לא ידוע לנו ולכל היותר ניתן לקבל את $M'' \; XOR \; M'$

כעת נזכיר כי הסגל מודע לנוסח המקורי M ומודע לדף הסופי "M

6. **<u>זיהוי השינויים עב 4:</u>**

מידיעת "M ניתן למצוא בעזרת XOR פשוט את K עם תחילת ההודעה השנייה ולאחר מכאן בעזרת XOR פשוט של תחילת ההודעה הראשונה עם K למצוא את 'M. כעת כשאנחנו יודעים את כל הM ניתן לדעת מי עשה את השינויים => שינויים מהנוסח הסופי "M לM' הם אלו שבוצעו על ידי בוב. ושינויים שבוצעו מM' לM הם שינויים שבוצעו על ידי אליס. ועל כן ניתן לזהותם.

7. **<u>זיהוי השינויים עב 5:</u>**

מידיעת "M ניתן למצוא בעזרת XOR פשוט את K עם תחילת ההודעה השנייה ולאחר מכאן בעזרת XOR פשוט של תחילת ההודעה הראשונה עם K למצוא את 'M. לכן באופן דומה לסעיף הקודם ניתן לחשב את השינויים גם פה.

8. **<u>זיהוי השינויים עב 3:</u>**

מהשיקולים שהוסברו ב3 ראינו שניתן לדעת את כל הM ועל כן ניתן למצוא את כל השינויים. כעת כשאנחנו יודעים את כל הM ניתן לדעת מי עשה את השינויים => שינויים מהנוסח הסופי "M לM' הם אלו שבוצעו על ידי בוב. ושינויים שבוצעו מM' לM הם שינויים שבוצעו על ידי אליס. ועל כן ניתן לזהותם.

9. **<u>זיהוי השינויים עב 5:</u>**

מהשיקולים שהוסברו בסעיף 5 לא ניתן לזהות את השינויים של אף אחד מכיוון שלמעט M המקורי לא ידוע לנו אף M אחר.