הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב סמסטר אביב תשפ״ב

הגנה ברשתות 236350

תרגיל בית מס׳ 6

הגשה: עד יום ד׳, 29/06/2022, 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 להדר (hadarsivan@cs)
בנוגע לשאלה 2 נא לפנות לטל (talneoran@cs)
בנוגע לשאלה 3 נא לפנות לעידן (idel@cs)

שאלה 1 – SSL

אוניברסיטת פרינסטרול רוצה לאפשר לסטודנטים שלה לגשת לשירותים שונים (כמו גיליון ציונים, שרת הגשת/החזרת עבודות וכו׳) בצורה מקוונת. היות שהם אינם מעוניינים שעבודותיו וציוניו של סטודנט יחשפו לעיניו של אף אחד פרט לסטודנט עצמו - החליטו מנהלי הרשת להשתמש בפרוטוקול דמוי SSL לאבטחת התעבורה לשרתים. הואיל והאוניברסיטה לא מעוניינת לרכוש סרטיפיקטים לכל השרתים הללו - הוחלט שכל סטודנט יתאם סיסמה (pass) מול השרתים וישתמש מולם בגרסה שונה של SSL, שתקרא SDL. הפרוטוקול החדש נראה כך:

1: ClientHello(version, cipher_suites, client_random) →

2: ← ServerHello(version, cipher_suite, server_random), ID_S, $g^x \bmod p$

3: ID_c, $E_{f(pass)}(g^y \bmod p)$, E_k(pre_master_secret) →

ChangeCipherSpec →

4: FinishedClient →

← *ChangeCipherSpec*

5: ← FinishedServer

הפרוטוקול SDL זהה ל- SSL, פרט לשינויים הבאים:

- ה-sid לא נשלח (אין הפעלה מקוצרת של הפרוטוקול)
- אף אחד מהצדדים לא מחזיק סרטיפיקט
- ID_C ו-ID_S הן מחרוזות המזהות את הלקוח (הסטודנט) ואת השרת בהתאמה
- בהודעה 2 השרת שולח מפתח DH: $g^x \bmod p$ (כאשר x ידוע רק לשרת)
- בהודעה 3 הלקוח שולח מפתח DH מוצפן תחת מפתח הנגזר מסיסמתו: $E_{f(pass)}(g^y \bmod p)$ (כאשר y ידוע רק ללקוח)
- בהודעה 3 pre_master_secret מוצפן תחת המפתח $k = f(g^{xy} \bmod p)$
- E הינה פונקציית הצפנה סימטרית בטוחה ו-f היא פונקציית תמצות בטוחה כלשהי.

1. האם הפרוטוקול מקיים את תכונת ה- PFS (Perfect Forward Secrecy)? בתשובתכם הסבירו מהי הסיסמה ארוכת הטווח והסיסמה קצרת הטווח.
2. בסעיף זה, הפרוטוקול יקרא בטוח אם תוקף אקטיבי לא יכול לקרוא מידע ששולח השרת ללקוח לאחר סיום ה-SDL ולא יכול להתחזות ללקוח ולבקש מידע כזה בעצמו. האם הפרוטוקול בטוח לפי הגדרה זו? הניחו שהשרת מאפשר מספר קטן מאוד של ניסיונות התחברות כושלים לפני שיחסום את המשתמש.

בסעיפים הבאים – תוקף יכול לראות את כל התעבורה בין השרת ללקוח (ובפרט – נניח כי יש לו כמה התקשרויות מוצלחות שהלקוח ביצע מול השרת בעבר). תוקף אקטיבי יכול, בנוסף, לנסות להתחזות לאחד הצדדים או לנסות ולהתערב בתעבורה ביניהם. לאחר 10 נסיונות התחברות לא מוצלחים מולם – גם השרת וגם הלקוח לא מוכנים להתחיל נסיונות התחברות חדשים (מספר הסיסמאות האפשריות של המשתמש גדול בהרבה מ- 20).

בכל אחד מהסעיפים הבאים, אם הפרוטוקול עמיד בפני התקיפה - הסבירו מדוע, ואם לא - הסבירו כיצד יוכל תוקף לבצע את התקיפה.

3. האם הפרוטוקול SDL עמיד בפני תקיפת מילון מצד תוקף פאסיבי?
4. האם הפרוטוקול SDL עמיד בפני תקיפת מילון מצד תוקף אקטיבי?
5. נניח שהודעות 4 ו- 5 מגיעות בסדר הפוך. כלומר, לאחר קבלת הודעה 3 השרת שולח את הודעת ה-Finished שלו (שמאמתת הפעם את הודעות 1-3), הלקוח מוודא אותה ואם הוידוא עבר בהצלחה - שולח את הודעת ה-Finished שלו (שמאמתת הפעם את הודעות 1-4).
האם הפרוטוקול לאחר השינוי הנ״ל עמיד בפני תקיפת מילון מצד תוקף אקטיבי?

שאלה 2 – IKE

מספר סטודנטים החליטו לערוך תחרות בנושא IKE, כשהמטרה היא ליצור פרוטוקול חדש ויעיל יותר מבחינת גודל ההודעות שנשלחות ברשת בין הצדדים שמריצים את IKE תוך כדי שמירה על תכונות האבטחה של IKE.
כדי להפוך את המשימה לקלה יותר, החליטו הסטודנטים להניח שהפרוטוקולים החדשים לא צריכים לתמוך במספר הפעלות של הפרוטוקול במקביל בין זוג נקודות קצה (הפעלה של הפרוטוקול תתחיל לא לפני שהפעלה קודמת של הפרוטוקול בין אותו זוג נקודות קצה הסתיימה).
בסעיפים הבאים יתוארו הצעות שעלו כחלק מהתחרות. עליכם יהיה לנתח ולקבוע עבור כל הצעה אילו מהבאים נכון עבורה.

A. ההצעה פוגעת בתכונות האבטחה של פרוטוקול IKE המקורי.
B. ההצעה לא פוגעת בתכונות IKE אך גם לא מקטינה את כמות המידע שמוחלף בין הצדדים.
C. ההצעה לא פוגעת בתכונות IKE ומצליחה להקטין את כמות המידע המוחלף.

בתחילת כל תשובה עליכם לציין תחילה את אחת מהאותיות A,B,C עפ"י בחירתכם. אם בחרתם A עליכם לציין במפורש בתשובתכם אילו תכונות של IKE המקורי נפגעות בהצעה, ואז לתאר התקפה שאפשר לבצע על הפרוטוקול המוצע ואי אפשר לבצע על IKE המקורי. אם בחרתם B או C עליכם לנמק מדוע השינוי שמופיע בהצעה לא פוגע בתכונות של IKE, ולאחר מכן לנמק את בחירתכם בדבר כמות המידע בפרוטוקול החדש ביחס ל-IKE.

1. לימור הציעה את פרוטוקול LIKE אשר זהה ל- IKE למעט השינוי הבא:
בהרצה של Main Mode, ב-header של ההודעות, ה- cookie יהיה בגודל ביט אחד.
2. בן הציע את פרוטוקול BIKE, אשר זהה ל- IKE למעט השינוי הבא:
בהרצה של Aggressive Mode, ב-header של ההודעות, לא ישלחו cookies. בכל מקום אשר נדרש לצורך החישוב ערך ה- cookie נשתמש בערך 0.
3. נירית הציעה את פרוטוקול NIKE, אשר זהה ל- IKE למעט השינוי הבא:
בהרצה של Quick Mode, השדה M-ID לא יישלח בהודעות הפרוטוקול (במקומו נשתמש בערך 0).
4. אבי הציע את פרוטוקול IKEA, אשר זהה ל- IKE למעט השינוי הבא:
בשלב אימות הצדדים, מיד לאחר שכל צד מחשב את מחרוזת ה HASH שלו כפי שמתואר ב-IKE, המחרוזת תתומצת שוב – $HASH = PRF_{SKEYID}(HASH)$

שאלה 3 – Wireless

1. גברת פלפלת החליטה לממש ברשת שלה את פרוטוקול האימות הבא, בהתבסס על ארכיטקטורת 802.1X, אותו היא כינתה BREAP:

Supplicant		Authentication Server
EAP-Start	→	
	←	**EAP-Request/Identity**
EAP-Response/Identity	→	
	←	**EAP-Request/BREAP,** $Challenge_{AS}$
EAP-Response/ $E_{Pub_{AS}}(Password_{Supplicant} \parallel Challenge_{AS} \parallel Challenge_{Supplicant})$	→	
	←	**EAP-Request/** $Sig_{Priv_{AS}}(Challenge_{Supplicant})$
EAP-Success/Failure	→	
	←	**EAP-Success/Failure**

כאשר:

- $Challenge_{AS}$ הוא ערך אקראי בן 128 ביט שמגריל שרת האימות
- $Challenge_{Supplicant}$ הוא ערך אקראי בן 128 ביט שמגריל המחשב המתחבר
- $Password_{Supplicant}$ היא סיסמא סודית שכל Supplicant תיאם באופן מאובטח עם שרת האימות
- Pub_AS הוא המפתח הפומבי של שרת האימות, הידוע לכל שהועבר באופן מאובטח
- Priv_AS הוא המפתח הפרטי של שרת האימות, הידוע רק לו
- E מסמל הצפנה באמצעות RSA
- SIG מסמל חתימה על תמצות ההודעה באמצעות RSA.[1]
- עם סיום ריצת הפרוטוקול בהצלחה, שרת האימות מעביר ל-Authenticator את המפתח המשותף:

$$PMK = Challenge_{AS} \oplus Challenge_{Supplicant}$$

a. הסבירו כיצד הצדדים מאמתים האחד את זהותו של השני.
b. האם הפרוטוקול חשוף למתקפת מניעת שירות על שרת האימות? הסבירו.
c. אם הפרוטוקול מקיים את תכונת PFS (Perfect Forward Secrecy)? הסבירו.
d. האם הפרוטוקול בטוח? אם כן, הסבירו מדוע. אחרת, הדגימו מתקפה.
e. האם הפרוטוקול החדש מונע הצבה של נקודת גישה סוררת (rogue access point)? אם כן, הסבירו כיצד ניתן לגלות את הנקודה הסוררת. אם לא, פרטו כיצד תתבצע המתקפה.

[1] שימו לב כי שימוש באותו מפתח לאימות והצפנה אינו בטוח, ולכן לא נעשה זאת בפרוטוקול אמיתי

2. במסגרת שיתוף פעולה מקצועי, הגדירה גברת מומין ש-Supplicants יוכלו לקבל גישה לרשת שלה על בסיס תקשורת מול שרת האימות של גברת פלפלת דרך האינטרנט. אולם, עקב מגבלות טכניות, נתמכים רק פרוטוקולי EAP אשר לא מצפינים את התקשורת בין שרת האימות ל-Authenticator (לא רדיוס). בהיעדר ערוץ מאובטח בין שרת האימות ל-Authenticator, הראו מתקפה שתאפשר לתוקף לא מורשה לקבל גישה לרשת של גברת מומין.