Assignment 2

שאלה 1:

1. התוקף נקרא לו E יכול להאזין להודעות בין A ל-B, ולאחר שלב 3 כאשר A שולח הודעה ל-E, התוקף E ישלח לשרת את ההודעה הבאה: E->S: {A,E,{NB,KAB}KAS}KES, עם השם שלו וההצפנה שלו.

ויקבל חזרה את ההודעה: S->E: {NB,KAB}KES , עם המפתח KAB שהוא צריך מוצפן עם המפתח KES שהוא יכול לפתוח. כעת E מסוגל להאזין לתקשורת בין A ל-B.

1. היכולות הנדרשות מהתוקף E כדי להצליח במזימה שלו הן:
   1. דרך להאזין להודעות שעוברות בין A ל-B.
   2. צריך להיות מזוהה עם השרת אמון ובעל מפתח משותף איתו.
2. ניתן לתקן את הפרוטוקול כדי להתמודד עם המתקפה מסעיף א' אנו נוסיף הודעה של מי הנמען בהודעה המוצפנת שיוצאת מ-A ל-B: A->B: {B,NB,KAB}KAS , בכדי שהשרת אמון כשיפתח את ההודעה ידע האם יש שם בעיה או להמשיך כרגיל.

שאלה 2:

השינוי הנ"ל אינו בטוח, נתאר את ההתקפה שהתוקף יכול לעשות:

הרעיון הוא שהתוקף ישתמש ב-replay attack , ע"י כך שיקליט את כל השיחה בין הלקוח לשרת. לאחר מכן התוקף בעצמו יזום שיחה עם השרת ויסכימו על מפתחות סימטריים משלהם לתקשורת שזה שלבים 1 עד 6. לאחר מכן בשלב 7 התוקף במקום להגריל מחרוזת r ישלח את EncPKS(PreMasterKey) שהקליט מהשיחה בין הלקוח לשרת, לאחר פעולה זאת השרת ישלח לתוקף את PreMasterKey ובכך התוקף יחשב את KMAC,KENC עם ה-transcript שהקליט והKEY שקיבל הרגע. עכשיו E שמח כי הוא יכול להאזין לתקשורת המוצפנת בין הלקוח לשרת.

שאלה 3:

1. פעולות שצריך לבצע בשביל לבדוק את הסרטיפיקט:
   1. פתיחת ההודעה עם המפתח הפומבי של השרת ובדיקה ש- IDx == IDB , אם כן אז המפתח הפומבי לגיטימי.
   2. פתיחת החלק השני עם המפתח הפומבי של השרת ובדיקה ש- IDx == IDB , אם כן אז המפתח הפומבי לגיטימי ולכן ניתן לפתוח גם אותו עם המפתח הפומבי של השרת.
   3. פתיחת החלק השני עם המפתח הפומבי 𝑃𝑈𝐵𝑋 שקיבלנו ולאחר מכן חילוץ של IDx עם המפתח הפומבי של השרת ובדיקה ש- IDx == IDB , אם כן אז המפתח הפומבי.
   4. פתיחת החלק השני עם המפתח הפומבי של השרת, לאחר מכן חילוץ של IDx עם המפתח 𝑃𝑈𝐵𝑋 שקיבלנו ולאחר מכן בדיקה ש- IDx == IDB , אם כן אז המפתח הפומבי לגיטימי.
2. נתאר לכל סעיף האם בטוח או לא:

בתרגיל זה אף פרוטוקול לא בטוח, וסעיפים 1 ו-2 דומים בכל שלב לכן נרשום אותם פעם אחת פה ובכל סעיף נמשיך מהשלב השלישי:

1) A תשלח בקשה ל-B לקבלת סרטיפיקט דרך C

2) B יבקש מ-CA את הסרטיפיקט שלו וישלח ל-A דרך C

1. **הפרוטוקול לא בטוח** –

3) C תשלח הודעה ל-CA עם IDB ומפתח פומבי משלה PUBC ותשלח ל-A את מה שהשרת הצפין

4) A תפתח את ההודעה עם המפתח הפומבי של CA תוודא שה-ID נכון ותשתמש במפתח הפומבי של C להצפנת ההודעות שלה עם B

5) C שמחה ומאושרת כי היא רואה הכל

1. **הפרוטוקול לא בטוח**

3) C תשנה את החלק הראשון בהודעה למפתח הפומבי שהיא קיבלה מ-CA בחלק השני תשים את ה-ID המקורי של B שקיבל מהשרת ותשלח את זה ל-A

4) A תפתח את ההודעה עם המפתח הפומבי של CA תוודא שה-ID נכון ותשתמש במפתח הפומבי של C להצפנת ההודעות שלה עם B

5) C שמחה ומאושרת כי היא רואה הכל

1. **הפרוטוקול לא בטוח**

3) C תשנה את החלק הראשון בהודעה למפתח הפומבי שהיא קיבלה מהשרת, והחלק השני היא תצפין בעזרת המפתח הפומבי שלה ותשלח את זה ל-A

4) A תפתח את ההודעה עם הפומבי של C ואז עם הפומבי של CA תוודא שה-ID נכון ותשתמש במפתח הפומבי של C להצפנת ההודעות שלה עם B

5) C שמחה ומאושרת כי היא רואה הכל

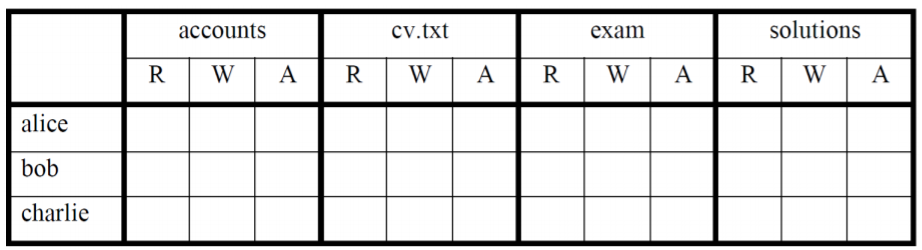
1. **הפרוטוקול לא בטוח**

3) C תשנה את החלק הראשון בהודעה למפתח הפומבי שהיא קיבלה מהשרת, ובחלק השני היא היא תשים את ההצפנה שלה של IDB עם ההצפנה שקיבלה מ-CA ותשלח את זה ל-A

4) A תפתח את ההודעה עם הפומבי של CA ואז עם הפומבי שקיבלה בשדה הראשון תוודא שה-ID נכון ותשתמש במפתח הפומבי של C להצפנת ההודעות שלה עם B

5) C שמחה ומאושרת כי היא רואה הכל

שאלה 4:



שאלה 5:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | manual.txt | report.txt | microedit | src/code.c | src/code/h |
| alex | R W \_ | R W \_ | R \_ \_ | R \_ \_ | R W \_ |
| benn | \_ \_ \_ | R \_ \_ | R W X | R W \_ | R W \_ |
| cloe | \_ \_ \_ | R W \_ | R \_ \_ | R \_ \_ | R \_ \_ |