הגנה במערכות מתוכנתות - ש.ב. 3

צפריר ריהן 039811880

גיא שקד 036567055

16 בדצמבר 2010

1. (א) אליס שולחת את $g^a \pmod p$ מוצפן לפי הסמא שלה. a נבחר באקראי והוא שונה בכל פעם שהפרוטוקול מופעל, לכן לתוקף אין דרך לדעת שהוא מצא את הסמא הנכונה - כיוון שאין הוא יודע מה אליס הצפינה באמצעותה.

(ב) אם איב הקליטה תקשורת בין אליס לשרת, וכן היא גילתה את a שבו אליס השתמשה בתקשורת הזו - איב יכולה לבצע התקפת מילון כדי למצא את הסמא של אליס. כדי לעשות זאת איב -

- תחשב $g^a \pmod p$ (g, p ידועים לכל, a ידוע לאיב)
- תעבור על הסמאות x מהמילון, ועבור כל אחת מהן -
  - תחשב $f(x)$ (f היא פונקציה ידועה לכל)
  - תחשב את $E_{f(x)}\left(g^a \pmod p\right)$, ותשווה לערך שאליס שלחה לשרת. אם הערכים שווים - הסמה של אליס היא קרוב לוודאי x.

(ג) גם לאחר השינוי הפרוטוקול איננו חשוף להתקפת מילון על הסמא של אליס. היתרון של איב כעת הוא שיש לה שני זוגות של טקסט גלוי ומוצפן, שהוצפנו באמצעות E על פי המפתח המשותף k, אנו מניחים כי פונקציית ההצפנה היא חזקה והתקפה שמשלבת שני טקסטים גלויים ומוצפני ידועים אינה ידועה, כך שלאיב לא תהיה דרך לגלות את המפתח k. מכאן - לאיב לא יהיה מידע נוסף בנוגע לסמא של אליס או להודעות שהוצפנו ומכילות את הסמא שלה, והתקפת מילון לא אפשרית - בדומה למצב ב-EKE רגיל.

(ד) לאחר שני השינויים ניתן לבצע התקפת מילון. ההתקפה תתבצע באופן הבא -

- לכל סמא x מהמילון איב תחשב את $f(x)$ ותבצע -
  - פענוח של $E_w(a)$ (נשלח בהודעה 1) על פי המפתח $f(x)$, את הערך נסמן ב-A
  - פענוח של $E_w\left(g^b \pmod p\right)$ (נשלח בהודעה 2) על פי המפתח $f(x)$, את הערך נסמן ב-$g^B \pmod p$
  - חישוב של $\tilde{k} \triangleq \left(g^B\right)^A \pmod p$ (העלאה בחזקה, מודולו p)
  - פענוח $E_k(challaenge_S)$ (נשלח בהודעה 2) על פי המפתח $\tilde{k}$, והשוואה ל-$challenge_S$ (נשלח בהודעה 3). אם הערכים שווים הסמא של אליס היא קרוב לוודאי x.

(ה) אם נעשה שימוש בצופן שטף או בצופן בלוקים שגודל בלוק קטן או שווה ל-$challenge$ במוד תפעול ECB (או דומה), תוקף יכול להתחזות לאליס או לשרת ולהשלים את תהליך ההזדהות (אבל - בסופו לא יהיה לתוקף וללקוח/שרת סוד משותף לצורך המשך הצפנת ה-session). נציג התקפה שבה התוקף מתחזה לשרת -

- אליס שולחת $E_w\left(g^a \pmod p\right)$.
- התוקף שולח מחרוזת אקראית במקום $E_w\left(g^b \pmod p\right)$ שהשרת היה אמור לשלוח, וכן מחרוזת אקראית נוספת בתור $E_k(challaenge_s)$, נסמן מחרוזת זו ב-C.
- אליס מפענחת את המחזורת האקראית הראשונה כאילו הייתה הודעה תקינה מהשרת, מחשבת לפיה k, ומפענחת על פיו את ההודעה האקראית השניה ומקבלת "אתגר" אקראי כלשהו. כעת היא מוסיפה אליו את האתגר שלה $challenge_c$ ומצפינה באמצעות k. כיוון שהבלוקים המוצפנים של שני האתגרים אינם משפיעים זה על זה אליס למעשה שולחת $C||E_k(challenge_c)$.
- התוקף מסיר את C מההודעה שקיבל מאליס, ושולח לה בחזרה את $E_k(challenge_c)$.

תהליך ההזדהות הושלם בהצלחה, אך בהנחה ואליס מצפה להשתמש ב־k להצפנת המשך התקשורת בינה ובין השרת התוקף לא יוכל להמשיך ולפענח את ההודעות שהיא תשלח לו. באופן שקול תוקף יכול להתחזות למשתמש (שלב 3 הופך להיות פשוט - שרשור של $E_k\left(challaenge_s\right)$ ומחרוזת אקראית שתשמש כ־$E_k\left(challaenge_c\right)$), אך גם במקרה הזה תוקף לא יוכל להמשיך את התקשורת אם השרת יצפה למידע מוצפן על ידי k.

2.

3.

4.