

### הגנה במערכות מתוכנתות - ש.ב. 3

צפריר ריהן      גיא שקד  
039811880      036567055

22 בדצמבר 2010

1. (א) אליס שולחת את  $g^a \pmod{p}$  מוצפן לפי הססמא שלה.  $a$  נבחר באקראי והוא שונה בכל פעם שהפרוטוקול מופעל, לכן לתוקף אין דרך לדעת שהוא מצא את הססמא 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 הססמא של אליס. כדי לעשות זאת איב -

- תחשב  $g^a \pmod{p}$  (ידועים  $g, p$ ), לכל  $a$  ידוע לאיב)

- תעבור על הססמאות  $x$  מהמילון, ועבור כל אחת מהן -

- תחשב  $f(x)$  (היא פונקציה ידועה לכל)

- תחשב את  $E_{f(x)}(g^a \pmod{p})$ , ותשווה לערך שאליס שלחה לשרת. אם הערכים שווים - הססמא של אליס היא קרוב לוודאי  $x$ .

(ג) גם לאחר השינוי הפרוטוקול איננו חשוף להתקפת מילון על הססמא 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 לססמא של אליס או להודעות שהוצפנו ומכילות את הססמא שלה, והתקפת מילון לא אפשרית - בדומה למצב ב-EKE רגיל.

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

- לכל ססמא  $x$  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  $E_w(g^b \pmod{p})$  (נשלח בהודעה 2) על פי המפתח  $f(x)$ , את הערך נסמן ב- $g^B \pmod{p}$

- חישוב של  $\tilde{k} \triangleq (g^B)^A \pmod{p}$  (העלאה בחזקה, מודולו  $p$ )

- פענוח  $E_k(challenges)$  (נשלח בהודעה 2) על פי המפתח  $\tilde{k}$ , והשוואה ל- $challenge_s$  (נשלח בהודעה 3). אם הערכים שווים הססמא 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  $E_w(g^a \pmod{p})$ .

- התוקף שולח מחרוזת אקראית במקום  $E_w(g^b \pmod{p})$  שהשרת היה אמור לשלוח, וכן מחרוזת אקראית נוספת בתור  $E_k(challenges)$ , נסמן מחרוזת זו ב- $C$ .

- אליס מפענחת את המחרוזת 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  $E_k(challenge_s)$  ומחרוזת אקראית שתשמש כ- $E_k(challenge_c)$ ), אך גם במקרה הזה תוקף לא יוכל להמשיך את התקשורת אם השרת יצפה למידע מוצפן על ידי  $k$ .

2. (א) ייתכן שלשני משתמשים יופיע אותו מפתח פומבי.

המפתח הפומבי של של משתמש (למשל - אליס) נגיש לכולם, ולכן כל משתמש אחר (איב) יכול להחליף את המפתח הפומבי שמוצג בפרופיל שלה (איב) כך שיהיה זהה למפתח הפומבי שמופיע אצל אליס. בנוסף, אך בסבירות נמוכה עד זניחה, ייתכן ששני משתמשים הגרילו את אותו מפתח פרטי ולכן יצרו את אותו מפתח פומבי. אפשרות אחרת היא שבעל האתר יחליף את המפתח הפומבי שמופיע בפרופיל, לצרכיו הפרטיים, כפי שנתאר בהמשך.

(ב) השיטה לא בהכרח שומרת על סודיות ההודעות, נתאר התקפה שבעל האתר יכול לבצע -

ברגע שאליס מעלה מפתח פומבי לפרטיה באתר, בעל האתר שומר את המפתח הפומבי הזה אצלו, ומחליף את המפתח הפומבי שיופיע בפרופיל של אליס במפתח פומבי אחר, שהוא מכיר את המפתח הפרטי המתאים לו (המפתח הפומבי של בעל האתר).

כאשר בוב ישלח הודעה לאליס - ההודעה עוברת דרך בעל האתר, הוא יפענח אותה ע"פ המפתח הפרטי שלו (שכן בוב הצפין אותה על פי המפתח הפומבי שלו, שהופיע בפרופיל של אליס), בעל האתר יקרא את ההודעה ואז יצפין אותה לפי המפתח הפומבי המקורי של אליס ויעביר אותה אליה. אליס תקבל את ההודעה של בוב, מוצפנת ע"פ המפתח הפומבי שהיא בחרה.

(ג) אין שיטה שתוכל להבטיח שא' ו-ב' שאינם מכירים זה את זה, כל אחד מהם בנפרד, אכן הבעלים של המפתח הפומבי שמוצג בפרטיו האישיים מבלי שיחלקו מראש סוד משותף או שיקבלו עזרה מצד ג' כלשהו (או מהאתר). כל פרוטוקול שנציע שאינו מבוסס על גורם אמין מאשר חשוף להתקפת man in the middle, לכן בעולם האמיתי יש צורך ב-CA.

(ד) תעודה דיגיטלית (certificate) היא מחזורת המכילה - זיהוי של המשתמש (שם משתמש), המפתח הפומבי שלו, תאריך תפוגה (של התעודה), שם ה-CA המנפיק וחתימה של ה-CA המנפיק על כל השדות הללו.

תפקידה של התעודה הוא לאפשר למשתמש (אליס) לוודא שהמפתח הפומבי של משתמש אחר (בוב) אכן משוייך לבוב ולא לגורם זדוני אחר שהחליף את המפתח הפומבי של בוב. אליס סומכת על ה-CA ועל כן הזיהוי של בוב באמצעות חתימה של ה-CA מאפשרת לה לדעת שזה הוא אכן המפתח הפומבי הנכון.

(ה) על מנת שה-CA יהיה אמין בעיני משתמשי הוא חייב לוודא את הזהות של המשתמשים להם הוא חותם על התעודות. הגורם המאשר עוקב אחרי תעודות שאינן אמין (כי המפתח הפרטי התגלה, למשל) ומפרסם CRL שמכיל רשימה של כאלו.

(ו) על פי רמת האבטחה הנדרשת - המשתמשים יוכלו לפגוש פיזית את נציג ה-CA ולאמת את המפתח הפומבי שלו, הם יוכלו להשתמש במנגנון PKI כדי לאשר את זהות ה-CA על פי זהותו של CA אחר שהם כבר מכירים וסומכים עליו (וחתם ל-CA החדש). לחילופין (אם לא נדרשת רמת וודאות גבוהה) יוכלו לסמוך על המפתח הפומבי של ה-CA שמופיע במקום ציבורי כלשהו וידוע לכולם.

(ז) בוב, שיוודע את המפתח הפומבי של ה-CA וסומך עליו (כפי שהוסבר לעיל) מקבל תעודה דיגיטלית שהונפקה עבור אליס, מפענח את החתימה שבסופה על פי המפתח הפומבי של ה-CA, ואם החתימה אכן תואמת לשאר השדות בתעודה הרי שהתעודה הונפקה לאליס על ידי ה-CA והמפתח הפומבי שמופיע בה הוא אכן המפתח הפומבי של אליס (אם התעודה טרם פקעה, ואינה מופיעה ב-CRL שפורסמו על ידי ה-CA).

(ח) ה-CA לא חייב להיות נגיש לצורך ווידוא אמינות התעודה (אלא רק לצורך יצירתה) - כפי שניתן לראות מאופן הווידוא שהוצג לעיל. אבל, אם בוב מעוניין לדעת בוודאות גמורה שהתעודה עדיין בתוקף ייתכן שהוא יהיה מעוניין לקבל את ה-CRL העדכני ביותר בזמן הווידוא, ולכן יהיה עליו לתקשר עם ה-CA.

(ט) שימוש באתר כ-CA אינו מוסיף לאמינות. כמו בסעיף ב' - כאשר בוב יבקש מהאתר את התעודה של אליס בעל האתר ישלח לו תעודה "מזוייפת" ובה המפתח הפומבי של בעל האתר (הוא יכול להכין תעודה כזו, כי הוא ה-CA). בוב יבדוק את אמינות התעודה ויקבל כי היא אמנה (בעל האתר הוא ה-CA), ולכן ישלח הודעה מוצפנת תחת המפתח הפומבי של בעל האתר. בעל האתר יפענח את ההודעה (על ידי המפתח הפרטי שלו), יעשה בה כרצונו, ולאחר מכן יצפין אותה על פי המפתח הפומבי האמיתי של אליס וישלח את ההודעה אליה - כך שהיא תוכל לפענח אותה.

נשים לב - אם אליס ובוב ישתמשו באמצעי תקשורת אחר (לא בהכרח בטוח, אבל כזה שאינו משתף פעולה עם האתר) על מנת להחליף תעודות - אליס תוכל לראות שהתעודה שהאתר ייצר עבור ונשלחת לבוב מכילה מפתח פומבי שונה, ומכך ללמוד שיש מי שמנסה לשבש את ההגנה על פרטיותם.

.3