הגנה במערכות מתוכנתות - ש.ב. 3

צפריר ריהן 039811880

גיא שקד 036567055

22 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 $E_{f(x)}(g^a \pmod p)$, 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 $E_w(g^a \pmod p)$.
- 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 $E_k(challaenge_s)$ ומחרוזת אקראית שתשמש כ-$E_k(challaenge_c)$), אך גם במקרה הזה תוקף לא יוכל להמשיך את התקשורת אם השרת יצפה למידע מוצפן על ידי k.

2. (א) ייתכן שלשנימשתמשים 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) שתי דרישות החלות על ה-CA הן-

- קיום דרישות מחמירות בתחום אבטחת המידע, כך שהמידע הפרטי של ה-CA לא יגיע לידיו של תוקף.
- עמידה בדרישות כלכליות, כך שמצד אחד ה-CA אינו בסכנה של פשיטת רגל, ומצד שני תוקף אינו יכול להשיג מידע פרטי על ידי מתן שוחד ותמריצים כלכליים.

(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, שיודע 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 אמינה (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. (א) נתאר התקפת מילון על פרוטוקול קרברוס הבסיסי:

- התוקף שולח הודעה "$ID_c, ID_s, nonce$" ל־KDC, כאשר ID_c הוא מזהה של הלקוח c שאת סיסמתו מעוניינים להשיג, ID_s הוא מזהה של שירות כלשהו, ו־nonce הוא מספר כלשהו שכמובן ידוע לתוקף.
- השרת מחזיר את ההודעה $(K_{c,s}, nonce)$ מוצפנת באמצעות מפתח המבוסס על הסיסמה של המשתמש. האופן שבו המפתח נגזר מסיסמת המשתמש ידוע לתוקף.
- התוקף מנסה לפענח את ההודעה שהתקבלה מהשרת באמצעות גזירת מפתח מכל אחת מהסיסמאות במילון. בכל נסיון, התוקף בודק אם ההודעה מסתיימת ב־nonce שהתוקף קבע – אם כן, בסבירות גבוהה, הסיסמה שניסה התוקף היא זו ש־c משתמש בה.
- ברגע שהסיסמה ידועה לתוקף, הוא יכול להתחזות למשתמש באופן שקוף לשרת.

אותם תנאים מתקיימים גם בפרוטוקול המלא, והתוקף יכול לפעול באותה צורה. למעשה, מאחר והמידע היחיד שדרוש לתוקף כדי להתחזות למשתמש לגיטימי הוא סיסמת המשתמש, אין חשיבות למידע שמוצפן על ידי השרת, ומבחינת התוקף הפרוטוקול הבסיסי והמלא זהים מבחינת התקפת מילון, מאחר ובשניהם nonce נכלל בהודעה המוחזרת למשתמש.

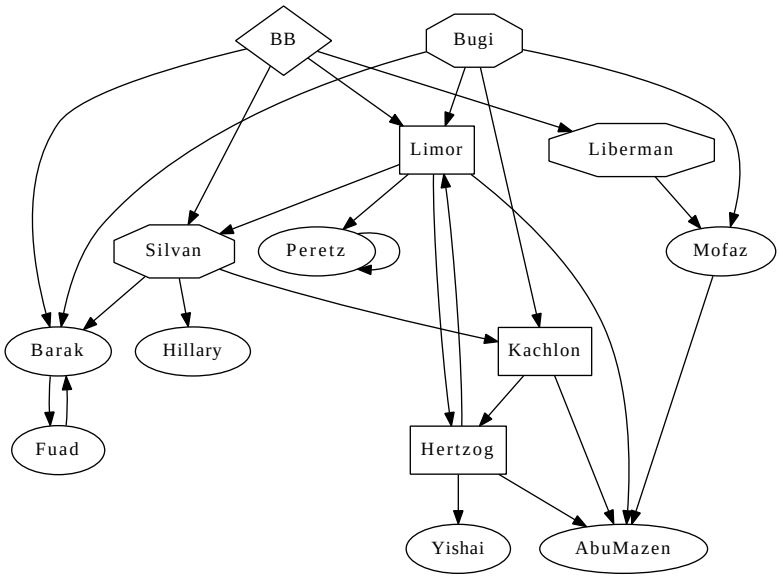
(ב) i. השינוי אינו פוגע בעמידות הפרוטוקול. למעשה, במימוש של קרברוס, ה־timestamp אכן משמש כ־nonce.

ii. השינוי מאפשר לתוקף להתחזות למשתמש לגיטימי ולקבל שירותים בשמו על ידי האזנה – התוקף מאזין לתקשורת בין הלקוח ל־TGS ומיירט את ה־Session Key, $K_{c,s}$. כעת ידועים לתוקף $K_{c,s}$, ID_c, timestamp, והוא מסוגל לייצר Authenticator לגיטימי. בנוסף, התוקף יירט את $Ticket_{c,s}$. באמצעותם, התוקף מזדהה מול השרת S בתור המשתמש c, ומקבל שירותים.

iii. גם שינוי זה מאפשר ל־c' להתחזות ל־c, באמצעות התקפת שידור חוזר – התוקף מאזין לתקשורת בין הלקוח לשרת S, ומיירט הודעת אימות כלשהי, שמכילה Authenticator שמוצפן באמצעות $K_{c,s}$, וכרטיס $Ticket_{c,s}$.
מכיוון שה־Authenticator אינו מכיל חתימת זמן, ו־$nonce_3$ הוא מחרוזת אקראית שאורכה חסום, לא ניתן לדרוש שה־Authenticator יהיה חד פעמי (דרישה זו תגרום לכך שמשתמש יוכל להזדהות רק 2^N פעמים, כאשר N הוא אורך ה־$nonce$).
התוקף כעת יכול לשדר את אותה הודעה ולהתחזות למשתמש c. ההתקפה תקפה כל עוד הכרטיס תקף (פרק זמן ארוך).

iv. אין פגיעה בעמידות הפרוטוקול – לאחר השינוי אין לתוקף מידע שלא היה בידיו קודם לשינוי.
עם זאת, לאחר השינוי אין לשרת דרך לדעת מהו $K_{c,s}$ ולפענח את ההודעה שהלקוח שולח, והפרוטוקול אינו שמיש.

4. (א) נבנה את מחזיק המפתחות של ביבי ־



כאן מעויין הוא ביבי עצמו (Ultimate trust), מתומנים הם מי שביבי סומך עליהם לחלוטין, מלבנים הם מי שביבי סומך עליהם באופן חלקי, וחץ מאליס לבוב מסמן שאליס חתמה על המפתח של בוב ושלחה לביבי.
כעת קל לראות ־

i. ביבי חתם ללימור סילבן וברק, לכן הוא המפתחות שלהם לגיטימיים.
אף אחד לא חתם לבוגי, לכן המפתח שלו לא לגיטימי.
ליברמן חתם למופז, ביבי סומך לחלוטין על ליברמן (והמפתח שלו לגיטימי), לכן המפתח של מופז לגיטימי.
סילבן חתם להילרי כחלון וברק, ביבי סומך לחלוטין על סילבן (והמפתח שלו לגיטימי), לכן המפתחות של הילרי כחלון וברק לגיטימיים.
רק ברק חתם לפואד, אבל ביבי לא סומך על ברק, לכן המפתח של פואד לא לגיטימי.
רק לימור (פרט לפרץ עצמו) חתמה לפרץ, אבל ביבי סומך על לימור רק באופן חלקי ולכן המפתח של פרץ לא לגיטימי.
כחלון ולימור חתמו להרצוג, ביבי סומך על שניהם באופן חלקי והמפתחות שלהם לגיטימיים - לכן המפתח של הרצוג לגיטימי.
רק הרצוג חתם לישי, אבל ביבי סומך על הרצוג רק באופן חלקי ולכן המפתח של ישי לא לגיטימי.
כחלון, הרצוג ולימור חתמו לאבו־מאזן, ביבי סומך על שלושתם באופן חלקי והמפתחות של שלושתם לגיטימיים - לכן המפתח של אבו־מאזן לגיטימי.

ii. ביבי חתם ללימור סילבן וברק, לכן הוא המפתחות שלהם לגיטימיים.
אף אחד לא חתם לבוגי, לכן המפתח שלו לא לגיטימי.
ליברמן חתם למופז, ביבי סומך לחלוטין על ליברמן (והמפתח שלו לגיטימי), לכן המפתח של מופז לגיטימי.
סילבן חתם להילרי כחלון וברק, ביבי סומך לחלוטין על סילבן (והמפתח שלו לגיטימי), לכן המפתחות של הילרי כחלון וברק לגיטימיים.
רק ברק חתם לפואד, אבל ביבי לא סומך על ברק, לכן המפתח של פואד לא לגיטימי.
רק לימור (פרט לפרץ עצמו) חתמה לפרץ, אבל ביבי סומך על לימור רק באופן חלקי ולכן המפתח של פרץ לא לגיטימי.
כחלון ולימור חתמו להרצוג, ביבי סומך על שניהם באופן חלקי ואבל $y = 3$ לכן למרות שהמפתחות שלהם לגיטימיים - המפתח של הרצוג לא לגיטימי.
רק הרצוג חתם לישי, אבל ביבי סומך על הרצוג רק באופן חלקי ובכל מקרה המפתח של הרצוג לא לגיטימי ולכן המפתח של ישי לא לגיטימי.
כחלון, הרצוג ולימור חתמו לאבו־מאזן, ביבי סומך על שלושתם באופן חלקי אבל רק המפתחות של כחלון ולימור לגיטימיים - לכן המפתח של אבו־מאזן לא לגיטימי (גם מופז חתם לאבו מאזן, אבל ביבי לא סומך על מופז).

(ב) שטרית מעוניין לגרם לביבי לחשוב שהמסמך נשלח מבוגי, לצורך כך הוא צריך לגרום לביבי לסמוך על מפתח פומבי (שקרי) של בוגי.

שטרית ייצר מפתח זו מפתח פרטי־פומבי חדשים, שישמשו אותו כמפתח פומבי־פרטי מזוייפים עבור שטרית, וכן זוג נוסף שישמשו אותו כמפתח פומבי־פרטי מזוייפים עבור סילבן.

כעת שטרית ישלח לביבי בשם סילבן חתימה על המפתח השקרי של שטרית, באמצעות המפתח השקרי של סילבן. ביבי סומך לחלוטין על סילבן, ואינו מוודא שהמפתח שבעזרתו נחתם האישור הוא מפתח לגיטימי (ואכן, הוא לא!), לכן ביבי מקבל את המפתח השקרי של בוגי כמפתח לגיטימי.

סילבן ישלח לביבי מסמך בשם בוגי, ויחתוך עליו באמצעות המפתח הפרטי השקרי של בוגי. המפתח מתאים למפתח הפומבי שהפך ללגיטימי בעיני ביבי, ולכן ביבי יאמין שהמסמך נשלח מבוגי.