ממ"ן 15 - שאלה 2

עמית בסקין 312259013

חלק I

Authentication Vulnerability

1 החולשה

בעת הירשמות לשרת, המשתמש מוסר לשרת שם לבחירתו ומקבל בחזרה מזהה ייחודי שמשמש אותו בבקשותיו העתידיות לשרת. בכל פעם שהמשתמש פונה לשרת הוא מזדהה באמצעות המזהה הנ"ל – כך השרת יודע באיזה לקוח מדובר ומה לעשות עם הבקשה. למשל כאשר לקוח מבקש לשלוף את ההודעות שנשלחו עבורו, כאמור הוא מזדהה עם המזהה הייחודי שקיבל מהשרת ומקבל בחזרה את כל ההודעות שמחכות לו. הבעיה היא שהמזהים הללו אינם חסויים ונגישים לכל משתמש שרשום לשרת. אכן בעת שליפת המשתמשים בשרת, הלקוח מקבל את רשימת המשתתפים לפי שמותיהם ומזהיהם הייחודיים – כך משתמש זדוני יכול להשתמש במזהים ייחודיים של משתמשים אחרים, להתחזות אליהם, לשלוח הודעות בשמם ולשלוף הודעות שמיועדות אליהם.

2 התקפה אפשרית

לאחר קבלת רשימת המשתתפים, התוקף בוחר משתמש X שהוא רוצה להתחזות אליו ושומר את המזהה הייחודי שלו כפי שהתקבל ברשימת המשתתפים מהשרת. לאחר מכן הוא יכול לשלוח מפתחות סימטריים לכל שאר המשתתפים בשמו של משתמש X. עתה, כאשר המשתמשים האחרים ישלפו את ההודעות שלהם, בין היתר הם ישלפו את ההודעה של המפתח הסימטרי מהתוקף, ישמרו אותו כמפתח שמשוייך למשתמש X, וכאשר ישלחו הודעה לשרת שמיועדת למשתמש X הם יצפינו אותה עם המפתח הסימטרי שקיבלו מהתוקף. לאחר מכן התוקף יכול להתחזות שנית למשתמש X בפני השרת ולשלוף בשמו את ההודעות שמיועדות אליו ואף לפענח אותן באמצעות המפתחות הסימטריים שהוא בעצמו שלח. כמו כן באותו האופן התוקף יכול לשלוח הודעות בשם משתמש X אל המשתמשים האחרים לאחר ששלח אליהם מפתחות סימטריים חדשים. הרי המשתמשים האחרים ישתמשו במפתחות הללו כדי לפענח את ההודעות שלכאורה התקבלו ממשתמש X ואכן יקראו אותן כהודעות שהגיעו מ- X עצמו כאשר למעשה התוקף הוא ששלח אותן.

3 הצעה לתיקון

נצפין את התקשורת בין השרת ללקוחות באופן דומה להצפנת התקשורת בין הלקוחות עצמם. נעשה זאת כך: ראשית נוסיף שדה נוסף לתחילת כל בקשה של לקוח לשרת. השדה הזה יהיה בגודל של בית אחד ויתחלק לשלוש אפשרויות:

קוד 3 – בקשת התחברות ראשונית.

קוד 5 – שליחת מפתח סימטרי לתקשורת עם השרת.

קוד 7 – לאחר שהלקוח כבר רשום, קוד זה יציין בקשה לשרת שיכולה להיות כל אחת מהבקשות בפרוטוקול המקורי.

כמו כן נוסיף קוד נוסף לתשובה אפשרית מהשרת: קוד 2005 – שליחת מפתח פומבי של השרת.

כעת, כשלקוח רוצה להירשם הוא יעשה זאת כמו בפרוטוקול המקורי רק שההודעה תתחיל עם קוד 3, ולאחר מכן הלקוח יצפה לקבל הודעה שמכילה את המפתח הפומבי של השרת (קוד 2005).

בשלב הבא הלקוח ייצור מפתח סימטרי ויצפין אותו באמצעות המפתח הפומבי של השרת. הלקוח ישלח את המפתח המוצפן אל השרת בהודעה שמתחילה עם קוד 5, ויחכה לאישור הרשמה כמו בפרוטוקול הרגיל. השרת יראה שמדובר בהודעה שמתחילה בקוד 5 ולכן ינסה לפענח אותה באמצעות המפתח הפרטי שלו. הוא יפענח את ההודעה, יקרא את המפתח הסימטרי שקיבל מהמשתמש וישלח תשובת אישור הרשמה כמו בפרוטוקול המקורי.

עכשיו, מעתה והילך, כאשר לקוח ירצה לשלוח בקשה לשרת, הוא יעשה זאת כמו בפרוטוקול המקורי אלא שכל הודעה תתחיל עם קוד 7 והכותרת שלה תוצפן על ידי המפתח הסימטרי שסוכם בין הלקוח לשרת בעת ההרשמה. כך כאשר השרת יקבל הודעה שמתחילה בקוד מספר 7, הוא יקרא את המזהה של המשתמש וכך יידע באיזה מפתח סימטרי להשתמש בשביל לפענח את הכותרת. דבר זה פותר את בעיית ההתחזות שכן עכשיו בשביל להתחזות למשתמש X התוקף צריך את המפתח הסימטרי ש־ X סיכם עם השרת, אך זה נשלח בצורה מאובטחת, מוצפן על ידי המפתח הפומבי של השרת, הרחק מהישג ידו של כל תוקף אפשרי. במידה שתוקף בכל זאת ינסה להתחזות למשתמש X על ידי שימוש במזהה הייחודי של X, כאשר השרת יקבל את ההודעה ויראה שהיא ממשתמש X, הוא ינסה לפענח את הכותרת עם המפתח הסימטרי שקיבל מהמשתמש X. אך מאחר שפעולת הפענוח תיכשל, השרת ישלח תשובת שגיאה וההתקפה תיכשל גם היא.

כמו כן, בשביל הפרטיות של המשתמשים, גם שארית הבקשה שלאחר הכותרת, יכולה להיות מוצפנת על ידי מפתח סימטרי. וכך גם התשובות של השרת למשתמשים יכולות להיות מוצפנות מהרגע שסוכם על מפתח סימטרי (גם כן בשני חלקים – הכותרת מוצפנת כחלק אחד והשארית מוצפנת כחלק שני). כך אף אחד לא יוכל להסניף את הבקשות והתשובות בין השרת למשתמשים ולאסוף מידע על התקשורת ביניהם.