ממן 15

# חולשה 1 – התחזות חלקית

החולשה הראשונה שמצאתי מאפשרת לתוקף להתחזות חלקית למשתמש אחר, לגלות פרטים על התקשורת שהוא מבצע, ולפגום בתקשורת שלו.

## מהלך החולשה

* קליינט זדוני מתחבר לשרת
* הקליינט מבצע הרשמה בתור משתמש חדש, ומקבל ID
* הקליינט מבקש את רשימת המשתמשים, ומקבל רשימה של משתמשים והID שלהם
* הקליינט שולח בקשת "שליפת הודעות ממתינות" (1004) **עם הID של משתמש תמים**

## תוצאות

* התוקף מקבל רשימה של הודעות שהתמים קיבל, ולמרות שהוא לא יכול לראות את התוכן שלהן הוא יכול לראות metadata שלהן ולגלות מי כותב הודעות לתמים ובאיזה אורכים.
* אם ברשימה הייתה הודעת "שליחת מפתח סימטרי" (2) לתוקף יש כרגע מפתח סימטרי לתקשורת עם קליינט אחר והוא יכול לשלוח לו הודעות מזוייפות ובאמצעות חזרה על השלב האחרון במהלך החולשה לקבל בסיכוי כלשהו הודעות שיוכל לפענח
* כל הודעה שהתוקף יקבל לא תגיע לתמים כי השרת יחשוב שהיא נקראה, ולמעשה יגרום למעיין DOS עבור המשתמש.

# חולשה 2 – הרעלת מפתחות

החולשה השנייה מאפשרת לתוקף לשלוח הודעות בשם משתמשים אחרים ובסיכוי קיים לקבל גם תשובות בשמם.

## מהלך החולשה

נגדיר קליינט זדוני ושני משתמשים תמימים – אליס ובוב.

* קליינט זדוני מתחבר לשרת
* הקליינט מבצע הרשמה בתור משתמש חדש, ומקבל ID
* הקליינט מבקש את רשימת המשתמשים, ומקבל רשימה של משתמשים והID שלהם (בין היתר של אליס ובוב)
* הקליינט מבקש את המפתח הפומבי של בוב.
* הקליינט שולח בקשת "שליחת הודעה ללקוח" (1003) בשם אליס אל בוב. ההודעה תהיה מסוג "שליחת מפתח סימטרי" (2) ותכיל מפתח סימטרי חדש מוצפן במפתח הפומבי של בוב.
* בוב שומר את המפתח הזה בתור המפתח הסימטרי שלו לתקשורת עם אליס.
* הקליינט שולח הודעות בשם אליס אל בוב מוצפנות במפתח הזה, ובוב מפענח אותן בתור הודעות מאליס.
* הקליינט שולח בקשת "שליפת הודעות ממתינות" (1004) עם הID של אליס וכל הודעה שהגיע מבוב תהיה עם מפתח שהוא מכיר ולכן יוכל לפענח אותן.
* בהינתן שהקליינט מושך הודעות חדשות באופן תכוף מספיק הוא יכול לעשות DOS לאליס ולהתחזות אליה מול בוב באופן מלא.

## תוצאות

התוקף מתחזה למשתמש בשרת אל מול משתמש אחר ומתכתב איתו.

# חולשה 3 – Man In The Middle

החולשה השלישית מאפשרת לתוקף (בצורה סטטיסטית אך אפקטיבית) לבצע MitM מלא לכל התכתבות שירצה בשרת.

## מהלך החולשה

נגדיר שוב את אליס ובוב אבל נשים לב שניתן לחזור על הפעולה הזאת עבור כל זוג משתמשים שנרצה.

* קליינט זדוני מתחבר לשרת
* הקליינט מבצע הרשמה בתור משתמש חדש, ומקבל ID
* הקליינט מבקש את רשימת המשתמשים, ומקבל רשימה של משתמשים והID שלהם (בין היתר של אליס ובוב)
* הקליינט מבקש את המפתח הפומבי של בוב.
* הקליינט שולח בקשת "שליחת הודעה ללקוח" (1003) בשם אליס אל בוב. ההודעה תהיה מסוג "שליחת מפתח סימטרי" (2) ותכיל מפתח סימטרי חדש מוצפן במפתח הפומבי של בוב.
* בוב שומר את המפתח הזה בתור המפתח הסימטרי שלו לתקשורת עם אליס.
* הקליינט מבקש את המפתח הפומבי של אליס.
* הקליינט שולח בקשת "שליחת הודעה ללקוח" (1003) בשם בוב אל אליס. ההודעה תהיה מסוג "שליחת מפתח סימטרי" (2) ותכיל **את אותו מפתח סימטרי כמו ששלח לבוב,** מוצפן במפתח הפומבי של אליס.
* אליס שומרת את המפתח הזה בתור המפתח הסימטרי שלה לתקשורת עם בוב.
* הקליינט שולח בקשות "שליפת הודעות ממתינות" (1004) עם הID של אליס ועם של בוב באופן תכוף ככל האפשר.
  + בכל פעם הקליינט עובר על ההודעות, בונה מכל אחת מהן בקשת "שליחת הודעה ללקוח" (1003) ושולח לשרת מחדש. כל הודעה חדשה מביניהן שהוא יכול לפענח הוא מפענח ושומר בצד.

## תוצאות

* התוקף רואה את כל התקשורת בין אליס ובוב, לפי הסדר ובזמן אמת
  + סטטיסטית כמובן, אם במקרה למשל אליס תמשוך הודעות בדיוק ברגע שבוב שלח אותן לפני שהתוקף מספיק אז הוא יפספס את ההודעה.
* התוקף ממשיך למשוך ולהחזיר את ההודעות לשרת עד שאליס ובוב מושכים אותן, ולכן אליס ובוב **לא חווים DOS ולא מודעים שיש בעייה או התערבות בתקשורת**

# פתרון

הפתרון שאני מציע עבור החולשות המתוארות הוא אימות הודעות ממשתמש על ידי השרת. כל הודעה ממשתמש אל השרת צריכה להיות בצירוף חתימה קריפטוגרפית באמצעות המפתח הפרטי של המשתמש. השרת יוכל לוודא אותה באמצעות המפתח הפומבי שנשלח אליו בעת ההרשמה ובכך לדאוג שרק המשתמש שביצע את ההרשמה יוכל לשלוח הודעות בשם הID הרלוונטי. כלל החולשות שתיארתי מסתמכות על היכולת לשלוח לשרת הודעות בשם משתמש אחר.