**מסמך מחקר: פרוטוקול MessageU**

**תיאור חולשות הפרוטוקול:**

**Man in the middle**

הפרוטוקול פגיע למתקפת man in the middle. זוהי התקפה בה התוקף מאזין לשיחה בין שני מחשבים, ומצליח להתחזות אליהם ובכך יכול להערים אליהם ולקבל גישה למידע רגיש.

**תיאור ההתקפה:**

נניח שברגע נתון, מחוברים לשרת שני לקוחות A,B והתוקף C מחובר גם הוא. התוקף C יכול לנצל הקמת תקשורת בין A לB ובכך להאזין להודעות העוברות ביניהם, אשר עלולות להיות סודיות באופן הבא:

בעת הקמת התקשורת לקוח A מבקש מהשרת את רשימת המשתמשים, התוקף C יכול להאזין לבקשה ולהגיב אליה לפני הסרבר, בתגובה התוקף ישנה את הID שמותאם לB ויחליף אותו בשלו, כך שלקוח A יחשוב שהוא מתקשר עם B אך בעצם יתקשר עם התוקף C

ברגע זה התוקף C יכול להאזין להודעות שA כאמור שולח לB, ויכול להגיב בהתאם ובכך לנצל את החולשה, ולמצוא מידע שעלול להיות קריטי.

**פתרון אפשרי:**

פתרון אפשרי הוא שימוש בTLS , אשר יכול להוות בסיס תקשורת מאובטח שימנע מצד מאזין שלישי לצוטט, ולהתחזות ללקוח אחר.

**distributed denial-of-service attack**

**תיאור ההתקפה:**

הפרוטוקול פגיע בנוסף למתקפת DDOS - distributed denial-of-service attack. התקפה בה תוקף חיצוני מייצר מספר רב של לקוחות שישלחו מספר עצום של הודעות באותו הזמן. השרת אינו מוודא את זהות הלקוח, ואינו מבקר על כמות הלקוחות, לכן הוא פגיע למתקפה זו.

בעזרת ההתקפה, התוקף יכול למנוע גישה לשרת משאר הלקוחות, או להאט את זמן התגובה של השרת ובכך לפגוע בתקשורת.

**פתרון אפשרי:**

פתרון אפשרי הוא יצירת מנגנון סינון אוטומטי היאפשר ניתור וזיהוי של משתמשים זדוניים, דבר זה יכול להתבצע באמצעות שאלות רנדומליות שיזהו שהלקוח שמתחבר הוא אדם ולא בוט.

מניעת החולשות:

man in the middle-

נוכל לקבוע מראש שלשרת יש מפתח פרטי ומפתח ציבורי שכל לקוח יודע מה הוא (כפי שהלקוח יודע לאיזה port להתחבר). נצפין את כל ההודעות שנשלחות בניהם עם מפתח סימטרי. בתחילת ריצת הלקוח, הוא ישלח לשרת מפתח סימטרי המוצפן על ידי המפתח הציבורי של השרת, שבו ישתמשו לתקשורת בין השרת ללקוח. השרת יפענח את המפתח הסימטרי בעזרת המפתח הפרטי שלו וכך השרת והלקוח יוכלו לתקשר בבטחה.

DDOS-

ניתן למנוע את ההתקפה בשני דרכים:

ליצור מנגנון אבטחה שיקשה על חיבור משתמשים זדוניים לשרת (סימון שאינך רובוט או זיהוי דברים בתמונה)

