פרויקט באבטחת מידע 236349

דו"ח פתיחה

מנחה: עמיחי שולמן

מתן גורן 206670549, נדב הלחמי 206784258

הקדמה

Apple משתמשים בפרוטוקול HAP- HomeKit Accessory Protocol שמאפשר חיבור מוצרי צד ג' שנמצאים בבית למכשירי Apple, ובאופן כזה לשלוט בהם. בנוסף ניתן להוסיף מכשירים נוספים שלא יועדו לשימוש ב Apple HomeKit באמצעות הרחבת HomeBridge.

מה אנחנו רוצים להשיג?

נרצה בתור תוקפים לאפשר את הרחבת סט המכשירים הידועים למערכת ה-HomeKit אצל מכשיר הקורבן כך שתתאפשר גישה של מכשירי התוקף אל המערכת הביתית או אל מכשירי הקורבן. נרצה לבחון את האפשרות של קבלת מידע מהמכשירים הביתיים ואת האפשרות להעמסת נתיב התקשורת על המכשירים הקיימים, ובכך לגרום להאטת השירות ואף לגרום ל-DoS. בנוסף, נבדוק את האפשרות של שליחת מידע אשר יגרום להרצת קוד זדוני.

למה זה טוב לנו?

על ידי ההבנה כיצד נוכל לגרום למכשיר נוסף (ולא מורשה) להתחבר למערכת הביתית ולנצל אותה על מנת להשתיל קוד זדוני, נוכל למנוע הישנות התקפות מסוג זה בעתיד ונוכל לרכוש מוצרים של Apple ללא חשש.

פירוט עבודה:

ראשית נרצה להבין את אופן פעולת המערכת ואיך אפשר להרחיב את סט היכולות המקומיות שלה, באמצעות שימוש במערכת Apple HomeKit או בסימולטור. בנוסף, נבדוק אפשרות להתחבר למערכת באמצעות מכשיר שלא יועד לה, תוך שימוש בHomeBridge למשל.

ננתח לעומק את פרוטוקול HAP, בפרט נייצר log של התקשורת, ונבחן את החבילות שעברו ברשת. נבין מי המכשירים הפופולריים יותר, ומה אופן הגישה הנפוץ אליהם, ומכך נסיק כיצד נוכל בתור תוקפים להתחבר אליהם. נחקור את אופן הצגת המכשירים המחוברים לרשת ונבדוק האם קיימת במערכת עדות להתחברות של המכשירים השונים, ונרצה להערים על המערכת ולשלוט במכשירים שמוצגים או לא מוצגים כמחוברים לרשת.

ננסה להבין את חולשות הפרוטוקול, בפרט נחקור חולשות למספר מכשירים רב באופן שידמה התקפת Botnet על המכשירים המחוברים לרשת באופן שיגרום למצב של DoS. נבין כיצד התקפה זו משפיעה על מכשירי המערכת ונבדוק האם ישנה אפשרות לנצל פרצה זו להשתלת קוד זדוני.

לוח זמנים:

27.3-3.4: נבין איך המערכת עובדת ונשווה אותה לאופן פעולת הסימולטור ו-HomeBridge.

3.4-16.4: נסמלץ מכשיר שאינו מיועד לתמוך בApple HomeKit ונבחן את השפעתו על המכשיר שלנו.

16.4-30.4: נייצר log של התקשורת ברשת הביתית בין המוצרים (אמיתיים ומדומים) למכשירים השולטים בהם ונחקור דפוסים חוזרים בו ואירועים מעניינים.

30.4-22.5: ננסה להשפיע על מכשיר הקורבן באמצעות המוצרים הנשלטים (אמיתיים ומדומים).

22.5-6.6: נבחן את התקשורת בין המכשיר שלנו אל המכשירים הקיימים במערכת ונבדוק איך ניתן לתקשר מבלי להשאיר עקבות במערכת.

7.6-30.6: נבדוק מהם המכשירים הנפוצים ביותר במערכת וננסה להפעיל כנגדם התקפת DoS, נבחן את השפעות ההתקפה. ננסה על ידי שימור בפרוטוקולים של המערכת להעביר מידע זדוני למכשירים הקיימים

(חודש יולי – תקופת מבחנים)

1.8-8.9: מימוש דמו שעובד על הסימולטור המריץ את ה-HomeKit.