מערכת הגנה יעילה על רשתות ה-GPS

למרות שנהוג לחשוב שמתקפות סייבר מגיעות רק דרך רשת האינטרנט, מתברר שגם מתקפות המשבשות, מטעות או חוסמות את מערכות ה-GPS נחשבות למתקפות סייבר לכל דבר ועניין. אלא שהחסימה הזו גורמת לנזק עצום למערכות GPS סמוכות ויכולה לשתק תעשיות שלמות. הסטארט-אפ GPSdome מצא פתרון לבעיה | **גליה היפש**

סו לדמיין את עצמכם נוהגים בעיר זרה. הצ־פיפות רבה, אתם צריכים לנווט ימינה ושמא־לה ברחובות לא מוכרים ומסתמכים אך ורק על תוכנת הניווט שלכם. לפתע המכשיר מפסיק את פעולתו ומודיע: אין קליטת GPS. מה עושים עכשיו? אז כשאתם נוהגים ברכב, אפשר לעצור בצד כמו פעם ולבקש מעוברי אורח הוראות הג־עה, אך מה קורה שמערכת GPS של אוניית משא מושבתת לפתע בלב ים? וזה בהחלט קורה.

ניסיון הטעייה (Spoofing) של מערכות ה-GPS

זה קרה למשל בסוף חודש יוני האחרון לקברניט של ספינה אמריקאית ששטה בים השחור, שגילה לתדהמתו שמערכת הניווט של האונייה מצביעה על כך שמיקומה הוא בכלל בשדה התעופה של העיר סוצ'י ברוסיה, כ-32 ק"מ בתוך היבשה. הקברניט מיהר לבדוק את העניין עם ספינות אחרות ששטו באזור, והתברר שכל מערכות ה-GPS באותן ספינות הראו את אותו מיקום: לטענתן הספינות נמצאות בשדה התעופה סוצ'י ולא בלב הים. עכשיו נסו לנווט כך אונייה במסלולה.

מדובר היה בניסיון הטעייה (Spoofing) של מערכות ה-GPS שעליה היו אחראים כנראה גורמים ברוסיה. זוהי רק מתקפת GPS אחת מיני רבות, לא כולן מתפרסמות בתקשורת. למרות שנהוג לחשוב שמתקפות סייבר מגיעות רק דרך רשת האינטרנט, מתברר שגם מתקפות המשבשות, מטעות או חוסמות את מערכות ה-GPS נחשבות למתקפות סייבר לכל דבר ועניין.

הסטארט-אפ הישראלי המסקרן GPSdome (כיפת הגנה ל-GPS) פיתח פתרון בדיוק עבור הבעיה הזו. **משה קפלן**, מנהל הטכנולוגיה הראשי (CTO) של החברה, מסביר: "פיתחנו מכשיר שיודע להתגבר הן על חסימת GPS רגילה והן על ניסיונות הטעייה שכוללים שינוי מיקום וזמן. מערכות ה-GPS האזרחיות בהחלט חשופות

משה קפלן | צילומים: יח"צ

לניסיונות של תקיפות סייבר, אולי למעט המערכות הצבאיות ששם מנגנוני ההגנה טובים יותר".

מדוע רוב תעשיית הסייבר מתרכזת במוצרים המגנים על תקיפות דרך רשת האינטרנט?

"כל יצרני ומתכנני המערכות להגנה מפני מתקפות סייבר מניחים שהכניסה למאגרי הנתונים או לארגון תיעשה דרך רשתות הנתונים ולכן הם מייצרים מערכות הגנה הבנויות מתוכנה. זה כמובן דבר שנכון לעשותו. ההבדל המרכזי הוא שברשת נתונים יכול האקר לשבת בפקיסטן, למשל, ולפרוץ למחשב בישראל או בארה"ב. לעומת זאת, כשמדובר ברשת GPS, כדי לשבש את התהליכים ולעשות Spoofing צריך להיות בקרבה פיזית יחסית למערכות. אי-אפשר לעשות את זה ממש מרחוק. צריך להתקרב פיזית ולכן להאקרים זו פרצה שאולי קוסמת פחות, אולם זו זירה פעילה מאוד".

אז מהיכן מגיעה הסכנה האמיתית למערכות ה-GPS?

"יש לא מעט אנשים שמסתובבים עם חוסמי GPS מתוך רצון להזיק או מתוך רצון שלא יעקבו אחריהם. נהגי מוניות או נהגי משאיות, למשל, שלא רוצים שמנהל צי הרכב שלהם יראה כל הזמן היכן הם נמצאים, שמים חוסם GPS, שאותו ניתן לרכוש ברשת בקלות בכמה עשרות דולרים, ונעלמים למספר שעות לבוסים שלהם. זה שאותו אדם חוסם את עצמו, זה חצי צרה, אלא שלמכשיר יש טווח חסימה של כמה מאות מטרים והוא יכול לחסום במקביל כמה מערכות אחרות. דוגמא אחת לכך היא שבשדה התעופה ניוארק בארה"ב נהג משאית הפעיל חוסם כדי שלא יעקבו אחריו, אך החוסם השבית את מערכת הניווט הקרקעית של שדה התעופה למשך כשבוע. הבורסה בלונדון הושבתה בזמנו ל-24 שעות בגלל חסימת GPS של מישהו בסביבתה. מחקר שנעשה בלונדון גילה שבכל רגע נתון מופעלים בעיר 10 אלפים חוסמי GPS, רובם מתוך סיבות של רצון לשמירה על הפרטיות, חלקם מתוך רצון להזיק, אבל הנזק הסביבתי שנוצר הוא הבעיה. גם בלחימת טרור, האוייב יכול להפעיל חוסמי GPS ולמנוע מכוחות ההצלה להגיע ליעדם ובכך להשתמש בכלי הזה כלוחמה. בהרבה מדינות עולם שלישי משתמשים בחוסם GPS לביצוע שוד משאיות. השודדים נוסעים לצד המשאית, מפעילים חוסם ואז עוצרים אותה ואף אחד בצי הרכב לא יודע היכן היא. הם יכולים לשדוד אותה באין מפריע".

כיצד המוצר שלכם פותר את הבעיה?

"המוצר שלנו הוא קופסא קטנה עם שתי אנטנות משלו, הוא מתחבר למקלט ה-GPS והאנטנות שלו מחליפות את האנטנות של המכשיר המקורי וכך מסוגלות להגן על המקלט. הפתרון מבוסס על אלגוריתם בשם null steering שהוא בעצם אנטנה מסתגלת שבאמצעותה אנחנו מחלישים את עוצמת החוסם כך שהוא לא יפריע לנו. לדוגמא, אם יש חוסם שמצליח לחסום מטווח של 350 מטרים, המערכת שלנו תוריד את הטווח ל-3.5 מטרים בלבד וזה הבדל קריטי מאוד".

להשתלב ברכב האוטונומי

חברת GPSdome הוקמה על ידי יו"ר קבוצת פוקוס טלקום, אהוד שרר, שני בניו, עומר ואביעד שרר, וקפלן עצמו. כיום הם חמישה עובדים קבועים בחברה המעסיקים בנוסף גם קבלני משנה. מטה החברה נמצא באזור התעשייה הדרומי בקיסריה. החברה ייצרה ומכרה עד כה 30 יחידות הגנה על מקלטי GPS, היא נמצאת בהליך ייצור של כמה מאות יחידות נוספות לאור הביקוש.

"כיום יחידה בודדת נמכרת ב-2,000 דולר", מסביר קפלן, "ואם קונים כמות גדולה המחיר יורד ל-1,300 דולר, אך המחיר צפוי לרדת עם השיפור הטכנולוגי של המוצר. קיבלנו לאחרונה מהמדען הראשי אישור לפרויקט פיתוח בן שנה שבסופו נעמוד עם מוצר משופר שמחירו יהיה זול יותר ויוכל להגיע ל-500 דולרים".

מהי התוכנית שלכם לטווח הארוך?

"התוכנית שלנו לטווח הארוך היא להשתלב בתוך הרכבים האוטונומיים. שם זה כבר יהיה צ'יפ הגנה ולא קופסא כמו היום. הכל עניין של פיתוח והתקדמות. בעוד כשלוש שנים צ'יפ כזה יוכל לעלות 30-50 דולר, ואנחנו רושמים פטנט כבר עכשיו על הדור הבא של הטכנולוגיה. הנושא הזה הוא קריטי בתוך המכוניות האוטונומיות מכיוון שבנוסף לפונקציית הניווט, גם כל התזמון של היחידות בתוך הרכב מתבסס על מערכות GPS, כמו גם הדו-שיח בין הרכב לסביבה שלו, שחייב להתבסס על תזמון מדוייק מאוד, ותזמון כזה אפשר לקחת רק מרשתות GPS ולא מרשתות נתונים. כל מערכות הסלולר החכמות והמתקדמות בכל תחנת קליטה של טלפונים מתבססות היום על שעוני GPS, כך שחסימה כזו יכולה לגרום למערכת שלמה כזו לא לתפקד. מערכת הגנה טובה על רשתות ה-GPS היא הכרח לכך שכל תעשיית הרכב האוטונומי תתפתח נכון ובצורה בטוחה".

אתר החברה: www.gpsdome.com