איומים קיברנטיים על כלי תחבורה זעירה בישראל ובעולם

מאת אמיתי דן

הקדמה

החל משנת 2010, חוקרי אבטחה שונים מציגים עבודות רבות המדגימות חולשות אבטחה ברכבים, ואת הסיכונים הנובעים מכך. הרגולטורים לאט לאט נכנסו לתמונה, וכיום חברות רכב ארבע גלגלי, מבינות שאבטחת מידע, הינו משהו שצריך לקחת בחשבון כבר מזמן הפיתוח, עד לייצור ולאחר המסירה ללקוח, התקדמנו באופן יחסי.

יש שוק אחר, שפחות מודגש ולא קיבל עדיין מענה - כלי תחבורה זעירים בעלי מחשב, מערכות בקרה ושליטה ההופכים לפופולריים במהירות (קרי: קורקניטים חשמליים, אופניים חשמליים, רובוטים, סקייטבורדים חשמליים וכלים אחרים בעלי משקל נמוך מכלי רכב ארבע גלגלי), ומאפשרים לתקוף את המשתמשים בצורות שונות ובאופן המסכן חיי אדם.

באופן מהיר יחסית הרחובות התמלאו בקורקינטים של חברות שונות אשר מחוברים לאפליקציות, חלקן בתקשורת מקומית ואחרות עם ממשק אינטרנטי, סקייטבורדים ממונעים עם שלט אלחוטי ולקינוח ניתן לראות גם ניצנים של אלחוטי אופניים בעלי קישוריות שונות, חלק מייצור וחלק מחלקים המורכבים בסדנאות שיפור מקומיות.

בנוסף, דגמים שונים של רובוטים המיועדים למרחב הציבורי והפרטי יוצאים לרחובות, ולא ברור האם מישהו שאל את השאלה - האם יש צורך באבטחת סייבר בעולם התחבורה הזעירה?

כדי להבין את הצורך בעיסוק בנושא, אביא מספר דוגמאות.

מדובר על מערכת ייעודית נגד גניבות, המאפשרת השבתת מנוע בזמן נסיעה או בעמידה וזאת דרך אפליקציה, ולאחר הקלדה של מספר ה-VIN.

המערכת בנויה בצורה כזו במכוון, ומאפשרת לתוקף לא מתוחכם לנצל אותה לרעה. את המידע הראשוני קיבלתי, במהלך שיחה על טכנולוגיות סייבר לפני למעלה משנה. לאחר מחקר משלים ואימות נתונים, פניתי לחברה מספר פעמים ולא קיבלתי תגובה או אינדיקציה לטיפול בבעיות שהצבעתי עליהן. תקופה נוספת לאחר מכן, שכללה גם יידוע של רשות הסייבר, פרסמתי את המחקר.

חשוב להבין, ניצול חכם של פגיעות זו - מאפשר יצירת אזור פיזי המשבית קורקינטים מסוג זה, או מתקפה אישית נגד גורם מסויים המשתמש בכלי תחבורה של החברה, תוך שימוש במספר השילדה הספציפי שלו.

אפשר לקרוא למתקפה כזו Physical APT או להשאיל מילים מפעולות ביטחוניות או פליליות באופיין.

לקראת הפרסום של המאמר מצאתי משהו מעניין בפורום ישראלי מוכר:

> *16-04-2018 13:44 Bishu*
>
> "קניתי אתמול את ה-*Quick3 Super*, ויש לי שאלה שקצת מטרידה אותי. מתוך הרגל, באופניים חשמליים יש מפתח שבלעדיו אי אפשר לנסוע באופניים, נכון שזה לא מהווה נעילה משמעותית וזה עוד מכשול בדרך, אבל בקורקינט זה סה"כ ללחוץ ארוך על הכפתור האמצעי בצג... שזה קצת יותר קל מללכת ולהחליף סוויץ' באופניים.
>
> נכון, יש את האפליקציה שדרכה אני יכול להפעיל מצב נעילה נגד גנבות, אבל זה גם מונע ממני לכבות את הקורקינט כי אי אפשר לעשות במצב הזה כלום, (תקנו אותי אם אני טועה) ומאיפה אני יכול לדעת שבנאדם שמכיר לא יוריד את האפליקציה ויתחבר לקורקינט שלי גם?"

הדבקה דרך עדכוני קושחה ו-modding פוגעניים

בדומה לתעשיית הרכב, גם בתחבורה זעירה החלו לצוץ סדנאות ופתרונות לשיפור רכב, החל מרמת המכלול, ועד לרכיבי חומרה מכנית דיגיטלית או קושחה. לדעתי האישית תופעות אלו, הינן חיוביות ומאפשרות למקסם את היכולות של המוצר, ולאפשר בעלות מלאה עליו, להגביר מהירות וכו'.

בו בזמן, שרשרת ההולכה של עדכוני קושחה אלו, בחלק מהיצרנים איננה מאובטחת ולכן תוקף פוטנציאלי יכול כיום בין היתר להפיץ עדכוני קושחה, המאפשרים להגביר את המהירות אך גם לתקוף את כלי הרכב - דרך עדכון נגוע.

דוגמא לכך, אפשר לקחת את הקורקינטים החשמליים של חברת Xiaomi, שבהם מעודכנים עדכוני קושחה לא רשמיים, תוך ניצול חולשת אבטחה במכשירים, למשתמש זה מאפשר בין היתר נסיעה מהירה יותר, לתוקף הפוטנציאלי זה יכול לאפשר להשתלט על אלפי קורקינטים ברחבי העולם.

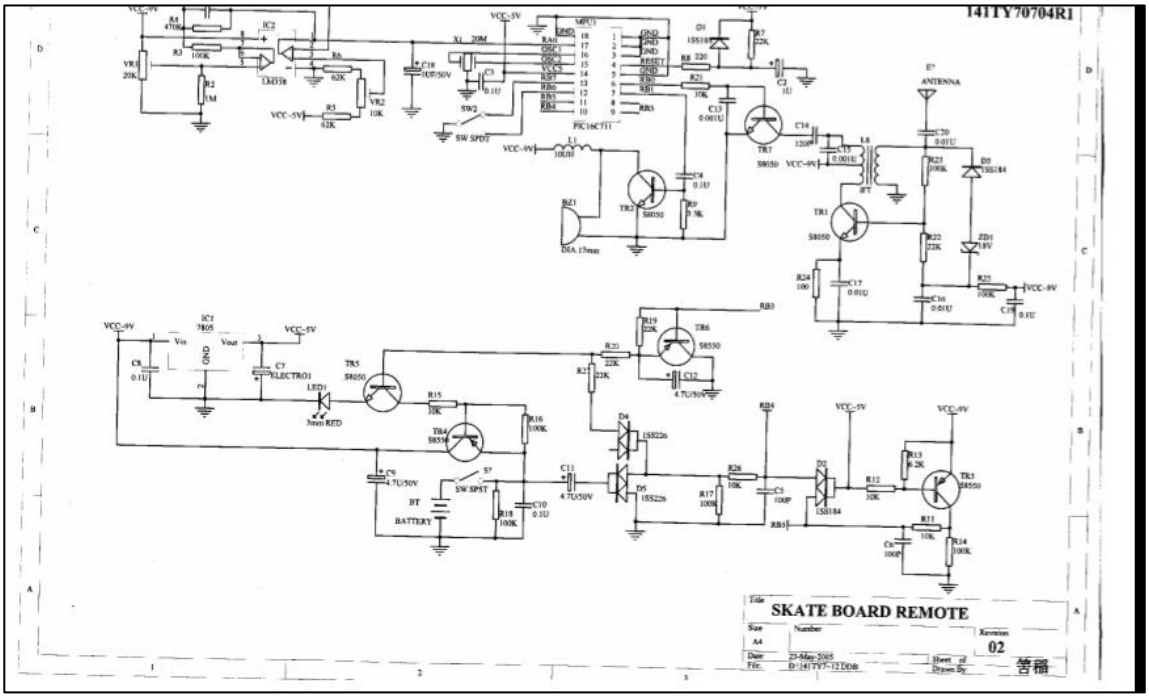
עדכונים אלו, יכולים לאפשר הדבקה נרחבת של קורקינטים שיאפשרו פגיעה באנשים, ולתוקף לשלוט בצבא של קורקינטים אופניים או רובוטים. ניתן לראות עדכונים לא פורמליים גם בכלים חד גלגליים אשר באופן הגיוני, תקיפות שלהם דרך עדכון תוכנה נגוע, יאפשרו יכולת פגיעה קטלנית ברוכב.

תקיפת שלט אלחוטי של סקייטבורד חשמלי

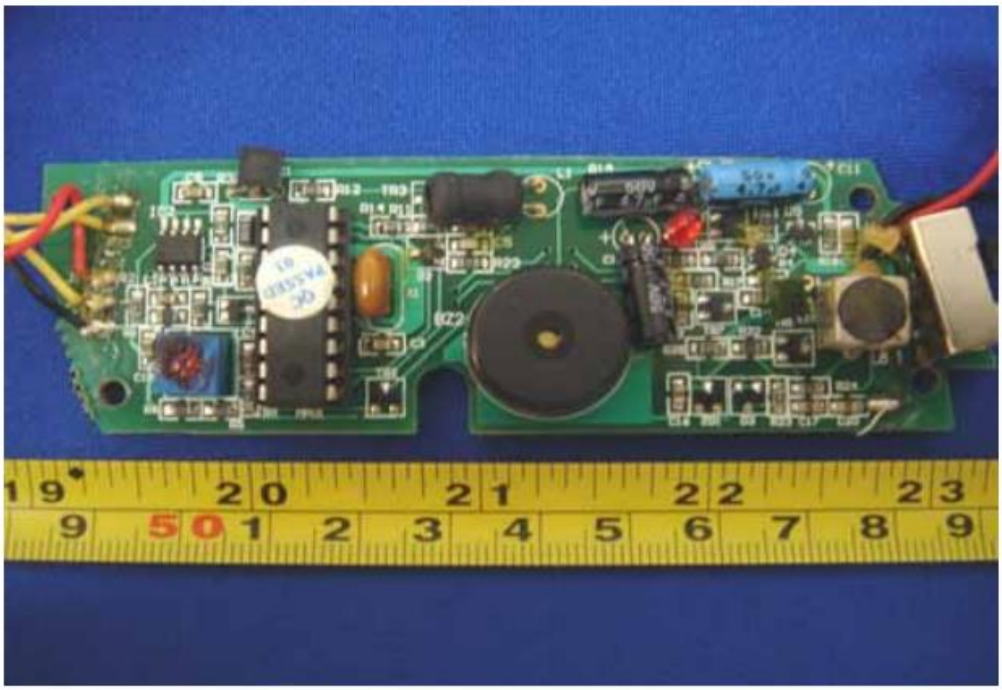
אמנם מדובר על כלים הנפוצים יותר במדינות אחרות, אבל גם בישראל ניתן לראות רוכבים המשתמשים בסקייטבורדים חשמליים, בעלי מצערת אלחוטית השולחת פקודות נסיעה ותאוצה לכלי הרכב באופן אלחוטי. חלקם מיוצרים בחו"ל ומיובאים לארץ, ואחרים מיוצרים על ידי בנאים מוכשרים בסדנאות ישראליות.

מימוש של תקיפה מוצלחת נגד כלים אלו, תאפשר מתקפות DDoS שבהם השידור ייקטע בפתאומיות, וכך גם היכולת לתת פקודות לכלי. בתרחיש אחר, התוקף ישתלט על השידור האלחוטי, ויתן פקודות תקיפה שיאפשרו לשלוח את העומד על בקורקינט למסלול התנגשות בטוח.

תוקף או חוקר אשר ירצה למצוא חולשות בשלטים, יוכל להתחיל את התקיפה על ידי חיפוש של אישורים רגולטוריים שהיצרנית קיבלה, לדוגמא - FCC. בחיפוש זריז, ניתן להגיע ל[קישור הבא]. בצורה זו, ניתן לאסוף בקלות מודיעין איכותי על התדרים בשימוש, המעגלים החשמליים, תוכניות, מגבלות שידור ועוד:



PCB - Component View



רק השבוע, הודגם כיצד גנבים פורצים רכב של טסלה, על ידי הגברת הטווח של ה-Keyless ולאחר מכן פתיחה של דלת. שיטות דומות יכולות לשמש גם במקרה שלנו.

מבט מסכם

להבנתי, יש כיום חוסר הבנה כאוטי, ואי אסדרה של תקינת סייבר בכלי תחבורה זעירים, מדובר על בעיה רחבה שלא נוגעת רק למדינת ישראל, אלא בבעיה הנוגעת לעולם התחבורה הזעירה באשר הוא.

בהקשר המקומי, אין ממש תקינה בישראל בהקשר של אבטחת סייבר של תחבורה זעירה הכוללת גם רובוטים ניידים.

רק בימים אלו נכתבת בעולם תקינת סייבר לרכבים עם ארבע גלגלים, כך שלמרות שכלי תחבורה יבשתיים כוללים על הנייר רובוטים קורקינטים וסקייטבורדים חשמליים, בפועל אין ממש מענה לפערים הללו מצד הרגולטור התקן והשוק, כאשר ניתן להבחין במעט חברות תחבורה זעירה ורובוטים, אשר מימשו אבטחה מסויימת מתוך החלטה עצמית, תקני בטיחות, התרעה של האקרים, עמידה ברגולציית פרטיות או צרכים כמו הגנה מפני הנדסה לאחור.

כלים אלו מציפים את הרחובות ומהווים מטרה נוחה לתוקפים עם מניעים שונים.

לדעתי המצב הזה צריך לאתגר אותנו כקהילה, ולדחוף לאיתור פרצות אבטחה, המלצות של פיתוח מאובטח של כלי תחבורה זעירים, עבודה מול רגולטרים ויצרניות ובאופן כללי לקיחת אחריות.

מראי מקום

מידע מודיעיני על חולשות בקורקינטים של Inokim:

https://www.fxp.co.il/showthread.php?t=18817105

הצגה של המערכת על ידי Inokim:

https://www.mivzaklive.co.il/archives/90661

מודינג שיאומי:

https://gist.github.com/losnir/78fae7e6cbb8cebf952bac8139beb258

פרסום מחקר אישי על חולשות ב-Inokim:

http://popshark11.blogspot.com/2017/11/an-anti-theft-system-allowing-attackers.html?m=1

https://seclists.org/fulldisclosure/2017/Nov/23

ביקורת על סקייטבורד חשמלי עם שלט:

https://youtu.be/lpx2zJOycXg

ליצירת קשר:

Linkedin - https://www.linkedin.com/in/amitay-dan-a63647aa

Twitter - https://mobile.twitter.com/popshark1

Blog - http://popshark11.blogspot.com/?m=1