OBDon't

מאת עומר כספי וליאור שרון

הקדמה

שימוש ברכיבי דיאגנוסטיקה לרכבים כיום, הינו נפוץ במיוחד כדי לנטר את מצב הרכב בזמן-אמת ולקבל אינפורמציה בנוגע לתקלות או נתוני חיישנים[1] של הרכב, רכיבים אלו הינם זמינים וזולים מאוד (כ-5 דולר לרכיב) ולפיכך נפוצים ונגישים. במאמר זה נסביר (על קצה המזלג) על מערכות הרכב הפנימיות הקשורות לאותו ממשק ועל סכנות האבטחה שבחיבור רכיב כזה לרכב.

מחבר OBD-II

OBD2 (ראשי תיבות של On Board Diagnostics II) הינו ממשק דיאגנוסטיקה ברכב אשר כחלק מהתקינה מחויב להיות בכל רכב אמריקאי משנת 1996, בכל רכב בנזין אירופאי משנת 2001 ובכל הרכבים אשר מיוצרים באירופה או מיובאים לאירופה משנת 2003, משמע שאם יש לך רכב ולא כרכרה, כנראה שיש לו ממשק OBD-II. התקינה בנוסף דורשת שהממשק לא יהיה במרחק העולה על חצי מטר מההגה ולא ידרוש שום כלים כדי להגיע אליו, המחבר נראה כך:

[1] סל"ד מנוע, מהירות, צריכת דלק

[מחבר OBD-II ברכב]

תפקידו של ממשק זה במקור היה לניטור ושליפת נתוני פליטה של מזהמים, והוא הפך להיות נקודת הכניסה העיקרית לאבחון תקלות ותקשורת כללית (כמו עדכוני תוכנה או הפעלת פונקציות כדי לאתר תקלות).

OBD Dongle

מאחר והתקן מגדיר פרוטוקול וממשק אחידים, ישנם רכיבים שהיום מאפשרים לקבל מידע על שגיאות ברכב בעזרת הטלפון ומתחברים אליו עם Bluetooth/WiFi, בפועל מה שרכיבים אלו מאפשרים זה לקבל מידע מהאוויר ולשדר אותו ברשת הפנימית של הרכב וההפך.

רוב רובם של ה-OBD Dongles (במיוחד הזולים) מבוססים חיקויים של צ'יפ שנקרא ELM327 אשר ה-Datasheet[2] שלו פתוח ונפוץ מאוד ברחבי הרשת. הם נראים כך:

[OBD Dongle לדוגמה]

ב-Datasheet אפשר לראות שאפשר לתקשר עם ה-ELM327 ב-AT commands המאפשרות לנו ליצור הודעות CAN כרצוננו או להאזין ולהודעות ולקרוא אותן. דונגל ה-OBD מתקשר עם מערכות הרכב בעזרת פרוטוקול פנימי בשם CANbus[3].

CANbus

פרוטוקול אשר תוכנן במקור לשימוש בכלי רכב ותעשיה. הוא בנוי להיות זול ליישום ועדיין לשמר רמת אמינות גבוה פרוטוקול זה הפך לסטנדרט בתעשיית הרכב ומשמש כדי לתקשר עם יחידות ECU[4].

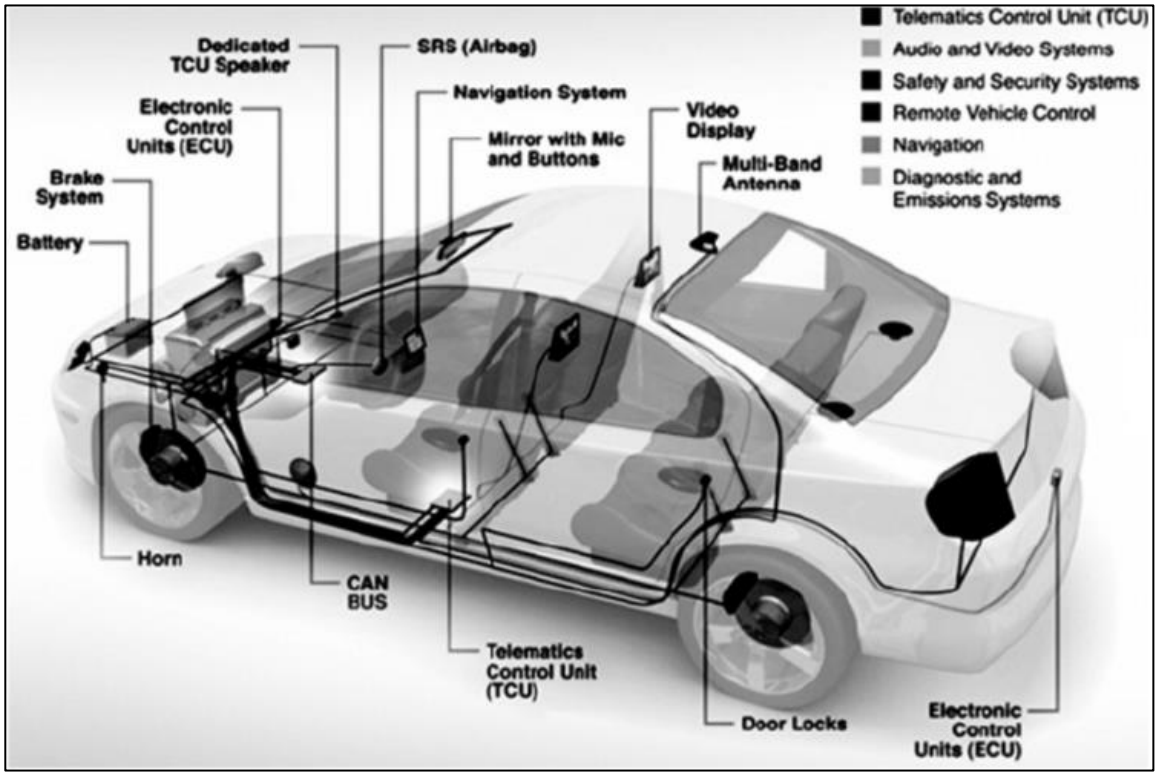
[2] Datasheet (או: דף נתונים) הוא מסמך שמסכם פונקציונליות של רכיב, ניתן למצוא את ה-Datasheet הספציפי בסוף המאמר

[3] CANbus - Controller Area Network bus

[4] - ECU יחידות שונות ברכב אשר שולטות על מגוון רכיבים ברכב כגון מנוע,בלמים, דלתות ועוד

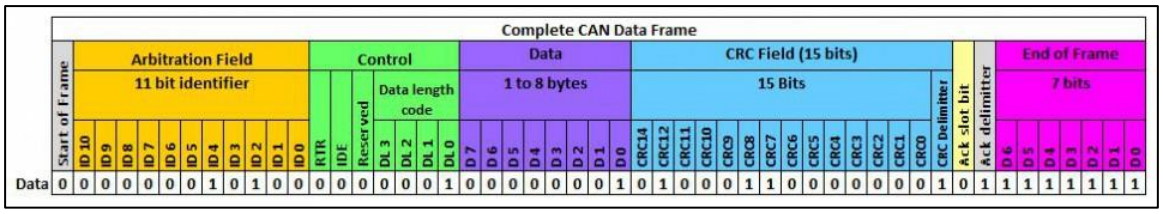
פרוטוקול זה בנוי בתצורת BUS, כלומר כל הודעה שנשלחת מגיעה לכל ה-ECU-ים שמחוברים לקווי הרשת.

דוגמא לרשת CAN טיפוסית:



[מקור: https://www.researchgate.net/figure/Typical-Automotive-CAN-Network_fig1_210264476]

מבנה של רשת CANbus ברכב

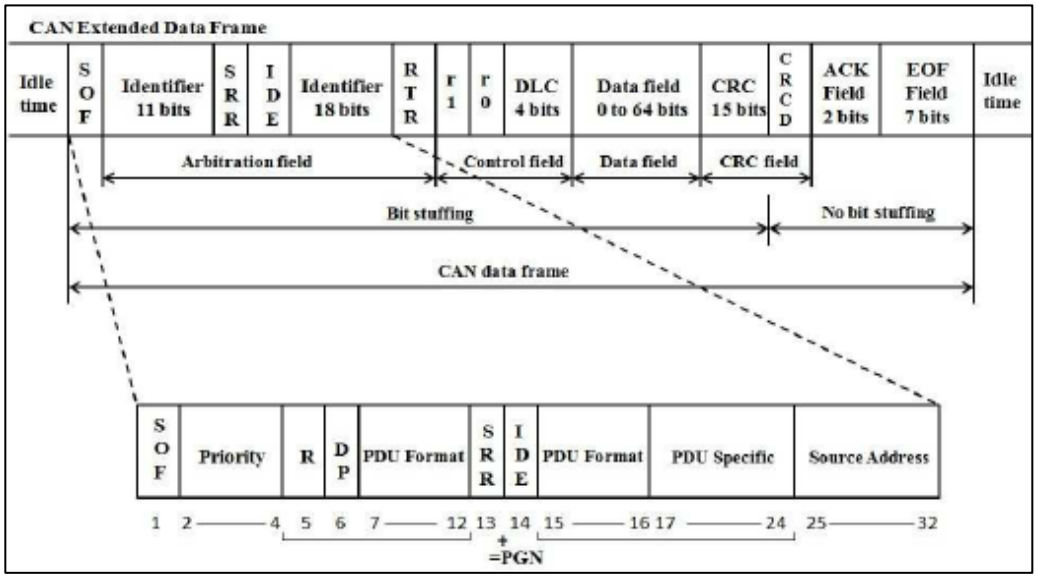


מבנה של חבילת CAN סטנדרטית

פירוט השדות:

1. Identifier - שדה אשר משמש כמזהה של ההודעה אך גם כעדיפות שלה, ככל שהמספר יותר נמוך ככה ההודעה בעדיפות גבוהה יותר
2. DLC - שדה המציין את גודל המידע שנשלח
3. Data - שדה אשר יכיל את המידע שנשלח
4. CRC - שדה המכיל את חישוב ה-CRC על ההודעה כדי לזהות שגיאות
5. Ack slot - שדה זה נשלח עם הערך 1 וכאשר יחידה מקבלת את הודעת ה-CAN היא בודקת האם ההודעה תקינה (על ידי בדיקה מול ה-CRC) ובמידה וההודעה תקינה מורידה את ערכו ל-0, כיוון שזהו BUS אין צורך לשלוח הודעה נוספת כדי לציין את קבלת ההודעה, בו זמנית השולח מאזין ל-BUS כדי לבדוק האם שדה ה-ACK הורד ל-0 וכך הוא יודע שההודעה התקבלה.

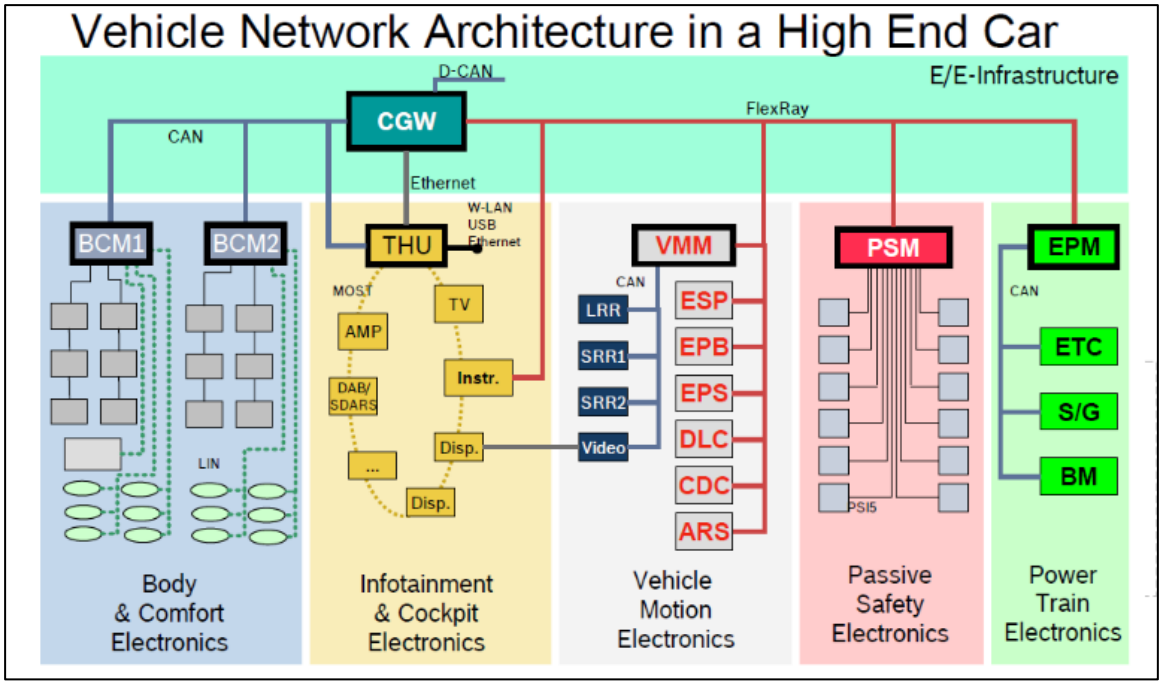
ישנה גרסה נוספת של CAN בשם Extended CAN שמרחיב את גודל הIdentifier ל-29 ביט. בנוסף, שדה בשם IDE[5] המציין שמדובר בהודעה מסוג Extended:



[5] IDE - Identifier Extension

מבנה חבילת Extended CAN

CAN BUS נוצר במטרה לחסוך בחוטים ולכן צריך לספק זמן תגובה נמוך ואינו מכיל מספיק מקום לשדה חתימה ולכן שיטות אבטחת תקשורת מקובלות אינן תקפות ברשתות מסוג זה.



האם שאלתם את עצמכם פעם איך רשת של רכב בנויה?

רכב היום בנוי מהרבה ECU-ים אשר לכל אחד תפקיד משל עצמו והם מתקשרים ביניהם במגוון פרוטוקולים (CAN, LIN, FLEXRAY, MOST, ETHERNET ועוד), כל קבוצה של ECU-ים מחוברת לתת רשת (אם הרשת שטוחה תת הרשת בעצם תהיה הרשת כולה), בין תתי הרשתות מנתב Gateway אשר תפקידו לקחת מידע אשר מגיע מרשת אחת ולנתב לרשת אחרת, לפעמים על מנת לעשות דבר זה יש להמיר בין הפרוטוקולים השונים.

Gateway הוא ציוד תקשורת ולכן מתפקד פוקציונלית בלבד ואינו כולל אמצעי אבטחה.

מהי הסכנה האבטחתית?

כעת לאחר שסקרנו כמה מושגים בסיסיים ואיך רשת של רכב בנוי נוכל להסביר למה OBD Dongle לא מאובטח הוא מסכן. כיוון שרוב ה-Dongle-ים מבוססים ELM327 קל מאוד לתקשר איתם ברגע שיש קישור Bluetooth ובעצם לשדר ולהאזין להודעות על ה-CANbus. הוכחה לכמה קל זה ניתן למצוא במסמך של ה-ELM327:

> The chip is now ready to send a message of your choosing. First, assign the header (ID bits) for your message. We'll use 777:
>
> ```
> >AT SH 777
> OK
> ```
>
> Now present the data bytes that you wish to send. We will provide these eight:
>
> ```
> >11 22 33 44 55 66 77 88
> ```

[AN07 - Sending Arbitrary CAN Messages]

הרוב המוחלט של ה-Dongle-ים לא מאובטחים כראוי ולא דורשים אימות כאשר מתחברים ב-Bluetooth או שהמכשיר מאפשר Pairing לא מאובטח. נושא אבטחת המידע בעולם ה-Automotive הוא נושא שנמצא בחיתוליו ולכן קיימים רכבים בהם לא שמו דגש על אבטחה בתכנון הארכיטקטורה של הרשת.

ניתן כמה דוגמאות כאלה:

- רכבים בהם הרשת can של הרכב היא רשת שטוחה כלומר אם תוקף השתלט על OBD Dongle סורר הוא יכול לתקשר עם המחשב מנוע או רכיבים קריטיים אחרים.
- רכבים בהם הרשת מחוברת על ידי gateway אשר משמש כראוטר בין תתי הרשתות השונות אך הוא לא אוכף שום אבטחה ורק מנתב בין הרשתות השונות לכן כמו במקרה הקודם עדיין נוכל להגיע מכל תת רשת לכל תת רשת

תופעה זו הופכת לעוד יותר בעייתית ברגע שמדברים על OBD Dongle-ים דוגמת הדונגלים אשר נמכרים כמו לחמניות ב-eBay, AliExpress ושאר ירקות ונכתב שתפקיד ה-Dongle לאבחן תקלות במנוע ומוכרים מעודדים את השארת ה-OBD Dongle מחובר כל הזמן למרות שחיבורו נצרך רק כדי לקבל מידע על תקלות (יצרני רכבים מגדירים שלא אמורה להיות תקשורת OBD בזמן נסיעה ותקשורת כזו עשויה להוות בעיית בטיחות).

יש אנשים שיטענו שווקטור תקיפה זה הוא לא סביר כיוון שהתוקף צריך להיות קרוב לרכב אך הוכח כבר במספר מחקרים שאפשר להאריך את הטווח של Bluetooth למספר קילומטרים ולכן תארו לכם מצב שבו תוקף משתלט על OBD Dongle של רכב בזמן נסיעה ומתחיל לתקוף את הרכב ולמשל מבטל את הבלמים, פתאום היעדר של אבטחת מידע יוצר מצב שעלול לגרום לסכנת חיים ובטיחות הנוסעים ברכב.

דוגמאות:

ברגע שלתוקף יש שליטה על מערכות קריטיות דרך ה-OBD Dongle הוא יכול לעשות שלל דברים; לדוגמא:

- לתת פקודה לפתוח את הדלתות. מכיוון שהרשת של הרכב פועלת וממשק ה-OBD מספק חשמל גם כאשר הרכב כבוי תוקף פוטנציאלי יכול לגנוב מכוניות או את תכולתן
- להשבית מרחוק מערכות קריטיות של הרכב בזמן נסיעה, ותאמינו לנו שאתם לא רוצים לדעת מה התשובה לתרגיל שכולל גוש מתכת שנע ב-100 קמ"ש ללא שליטה עם אנשים בתוכו

בנוסף התוקף פוטנציאלית יהיה מסוגל לבצע פעולות כגון:

- לחיצה על בלמים
- כיבוי מנוע
- התנעת מנוע
- פתיחת מנעול דלתות
- פתיחת תא מטען
- הפעלת צופרים
- שליטה ברדיו ומערכת הבידור
- ניתוק תיבת הילוכים (אוטומט)
- שינויי מצערת

מה ניתן לעשות כדי למנוע זאת?

נמליץ למשתמשים של Dongle-ים כאלה על צעדים שיוכלו לעזור כנגד פגיעויות אלה:

- לא להשאיר את ה-Dongle מחובר כשיוצאים מהרכב.
- לא לחבר את ה-Dongle בזמן נסיעה.

סיכום

במאמר זה הראינו איך במתארים מסוימים אבטחת מידע משפיעה לא רק על הנושאים הרגילים כגון פרטיות או סודיות אלא גם על המישור הפיזי ואיך פרצות אבטחה ברכבים יכולות לגרום לסיכון חיי אדם.

על המחברים

עומר כספי, מפתח אמבדד בתחום ה-Automotive Security בחברת GuardKnox שבזמנו הפנוי מתעסק במחקר חולשות לכל שאלה, הערה/הארה, מוזמנים לפנות אלי בכתובת:

komerk0@gmail.com

ליאור שרון, מפתח אמבדד בתחום ה-Network Security ועובד במשרה חלקית בחברת GuardKnox. לכל שאלה מוזמנים לפנות אליי בכתובת:

lior.sx@gmail.com

תודות

ברצוננו להודות לעידן נדב שנתן ייעוץ, הערות ותיקונים למאמר זה.

ביבליוגרפיה ומקורות נוספים לקריאה

- קישור לפריצה שבוצעה על ידי OBD Dongle פריץ:

https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

- ELM327 Datasheet:

https://www.elmelectronics.com/wp-content/uploads/2016/07/ELM327DS.pdf

- App Note 7: Sending Arbitrary CAN Messages:

https://www.elmelectronics.com/wp-content/uploads/2017/11/AppNote07.pdf