AVTOTRANSPORT VOSITALARINI KIBERHUJUMLARDAN HIMOYA QILISH BO‘YICHA YO‘L XARITASI

Abduraximov Ozodbek Azimjon o'g'li
Tojidinov Azizbek Ilhomjon o'g'li
Nazirjonov Ubaydulloh Nozimjon o'g'li
TATU Farg‘ona filiali talabalari

Annotation:*In this article, we will study the security issues of allowing external wireless communication. we will discuss security issues without the use of a defensive point of view and for each of the prevention, detection, deviation, countermeasures and recovery layers.*

Keywords:*CPS, ECU, OBD (onboard diagnostics).*

Annotatsiya: *Ushbu maqolada biz tashqi simsiz aloqaga ruxsat berishning xavfsizlik masalalarini o‘rganamiz. mudofaa nuqtai nazaridan foydalanga holda va har bir oldini olish, aniqlash, og‘ish, qarshi choralar va tiklash qatlamlari uchun xavfsizlik muammolarini muhokama qilamiz.*

Kalit so‘zlar:*CPS, ECU, OBD (bortli diagnostika).*

Avtomobil sanoati kundalik hayotimizning ajralmas qismiga aylandi. Avtotransport vositalarining rivojlanishi bilan avtomobilni boshqarish uchun birinchi navbatda mexanik echimlar asta-sekin avtomobil ichidagi kompyuter tarmoqlarini tashkil etuvchi elektronika va dasturiy echimlar bilan almashtiriladi. Rivojlanayotgan tendentsiya - avtomobil ichidagi tarmoqqa simsiz shlyuzni ulash orqali avtomobil domenida simsiz texnologiyani joriy etish. Simsiz aloqaga ruxsat berish orqali transport vositalari va infratuzilma va transport vositalari o‘rtasida real vaqt rejimida ma'lumot almashish haqiqatga aylanadi. Ushbu aloqa yo‘l holati haqida hisobot berish, qaror qabul qilish va masofaviy diagnostika va proshivkalarni havo orqali yangilash imkonini beradi. Biroq, tashqi tomonlarga avtomobil ichidagi tarmoqqa simsiz kirishga ruxsat berish kiberhujumlar uchun potentsial kirish nuqtasini yaratadi .

Avtomobil sanoati kundalik hayotimizning muhim qismiga aylandi va jamiyatimiz va turmush tarzimizning ulkan yaxshilanishiga olib keldi. So‘nggi bir necha yil ichida elektronika va dasturiy ta'minot avtomobilning yanada yaxshi ishlashiga hissa qo‘shdi . Zamonaviy avtomashinada avtomobil ichidagi tarmoq mavjud bo‘lib, u odatda 50-70 elektron boshqaruv blokidan (ECU) iborat bo‘lib, transport vositasini boshqarish va manevr qilish, navigatsiya va to‘xtashga yordam berish kabi ko‘plab funktsiyalar uchun javobgardir. Avtomobil ichidagi simsiz shlyuz avtomobil ichidagi tarmoq bilan tashqi aloqa uchun ishlatiladi. Rivojlanayotgan tendentsiyalar - real vaqt rejimida tirbandlik haqida ma'lumot berish, to‘qnashuvlar haqida ogohlantirish va dasturiy ta'minotni havo orqali yangilash imkonini berish orqali haydovchilarning xavfsizligi va qulayligini yaxshilash uchun transport

vositalaridan infratuzilmaga va avtomobildan avtomobilga aloqa . Shunday qilib, avtomobildagi hisoblash va aloqa jismoniy dunyodagi ob'ektlar monitoringi bilan birlashtiriladi, natijada kiber-fizik tizim (CPS) yaratiladi. Biroq, jismoniy dunyoning avtomobil ichidagi tarmoq bilan o‘zaro ta'siriga ruxsat berish bir qator xavfsizlik xavflarini keltirib chiqaradi, shu jumladan: avtomobilning funksionalligi va manevr qobiliyatiga qaratilgan kiberhujumlar . Shunday qilib, transport vositalarini ushbu hujumlardan himoya qilish zarurati paydo bo‘ladi.

Kiber-fizik tizimlar Avtotransport vositalariga kiberhujumlarning oldini olish uchun xavfsizlik yechimlari avtomobil CPS uchun ishlab chiqilishi kerak. Biroq, bunday echimlarni loyihalashda bir qator asosiy cheklovlar mavjud. Birinchidan, transport vositalari ichidagi ECU'lar hisoblash quvvati, xotira, tarmoqli kengligi va quvvat sarfida cheklovlarga ega. Ikkinchidan, ECUlar real vaqt rejimida ishlaydi, bu erda xabarlarning navbatda turishi va kechikishlarga yo‘l qo‘yilmaydi. Avtomobildagi sensorlardan olingan ma'lumotlar real vaqt rejimida qayta ishlanishi kerak va to‘g‘ri aktuatorlarga ta'sir qilish bo‘yicha qarorlar kechiktirmasdan qabul qilinishi kerak. Xavfsizlik echimlarini loyihalashda real vaqt cheklovlarini hisobga olish kerak. Uchinchidan, avtomobil aloqasi uchun trafik sxemalari an'anaviy IP tarmoqlaridagi trafik naqshlaridan farq qiladi. Masalan, avtomobil ichidagi tarmoqdagi CAN avtobusidagi ma'lumotlar translyatsiya qilinadi. Avtotransport vositalarining maxsus tarmoqlari avtomashinadan avtomobilga va transport vositasidan yo‘lga o‘tishda o‘z-o‘zidan shakllanishi mumkin edi. Bundan tashqari , avtomobil ishlab chiqaruvchilari transport vositalarida simsiz diagnostika va mikrodasturlarni yangilash uchun avtomobildan infratuzilmaga muhit yaratishi mumkin . Turli xil trafik shakllari va aloqa modellari turli xil echimlarni talab qiladi. Shunday qilib, IP tarmoqlari uchun ishlab chiqilgan an'anaviy echimlardan foydalanish mumkin emas

Avtomobil CPS uchun xavfsizlik yechimlarini ta'minlash bo‘yicha uchta eng muhim tadqiqot muammosi quyidagicha tasvirlangan. Avtomobil jismoniy dunyo bilan o‘zaro aloqada bo‘lishga imkon beradi, masalan, boshqa transport vositalaridan yoki chorrahalar va o‘tish joylaridan ogohlantirish signallarini qabul qilish. Natijada, jismoniy dunyoni taqlid qiluvchi kiberhujumlar sodir bo‘lishi mumkin. Shunday qilib, muammo avtomobilga kiruvchi ma'lumotlarning haqiqiyligini tekshirishdir. Masalan, transport vositasi qabul qilingan ogohlantirishning to‘g‘ri va yangi ekanligiga (takrorlanmaydi) va u to‘g‘ri jismoniy shaxsdan (masalan, transport vositasi yoki chorraha) yuborilganligiga ishonch hosil qilishi kerak. Kiruvchi ma'lumotlarning to‘g‘riligini tasdiqlash bir qiyinchilik bo‘lsa-da, tinglash interfeysini bosqinlardan himoya qilish boshqa vazifadir. Simsiz interfeys tinglash xizmati bo‘lganligi sababli, u o‘zgartirilishi va tajovuzkorga avtomobil ichidagi tarmoqqa kirishiga ruxsat berishi mumkin. Shunday qilib, tajovuzlarning oldini olish uchun tegishli mexanizmlarni ta'minlash muhim vazifadir. Ruxsatsiz kirishlarning oldini olish uchun xavfsizlik devorlari zarur va tajovuzkorlarni aniqlash va kuzatish uchun jurnallar va aniqlash mexanizmlari kerak. Biroq, ushbu xavfsizlik echimlarini real vaqt talablari va ECUdagi

cheklovlarni qondirish uchun loyihalash qiyin. Uchinchi tadqiqot muammosi - avtomobil ichidagi tarmoqdagi xavfsizlik echimlarini himoya qilish.

Faraz qilaylik, simsiz aloqa xavfsizligini ta'minlash uchun turli kriptografik kalitlar ishlatiladi va kirishni boshqarish roʻyxatlari faqat ruxsat berilgan ulanishlarga ruxsat berish uchun ishlatiladi, shuning uchun simsiz shlyuz hujumlardan himoyalangan. Tajovuzkor qurilmani avtomobilga jismoniy ulash orqali OBD (bortli diagnostika) porti orqali avtomobil ichidagi tarmoqqa kirishi mumkin . Agar xavfsizlik echimlari hujumlardan faqat simsiz shlyuz orqali himoya qilsa, tajovuzkor oʻrniga OBD orqali avtomobil ichidagi tarmoqqa hujum qilishni tanlashi mumkin. Masalan, tajovuzkor kerakli kriptografik kalitlarni osongina chiqarib olishi va simsiz shlyuz orqali kelajakdagi hujumlarni amalga oshirishi uchun kirishni boshqarish roʻyxatini yangilashi mumkin. Shunday qilib, avtomobil ichidagi tarmoqni va xavfsizlik ma'lumotlarini OBD orqali jismoniy hujumlardan himoya qilish qiyin.

Kiberfizik tizimlarida kelajakdagi ilovalar uchun gʻoyalar Ushbu boʻlimda biz keyingi 5, 10 va 20 yil uchun mumkin boʻlgan muhim bosqichlarni taqdim etamiz. Biz avtomobilsozlik sanoatiga yaxshi ma'lum boʻlgan chuqur mudofaa tamoyiliga muvofiq xavfsizlik echimlarini ishlab chiqishni taklif qilamiz . Keyingi 20 yil davomida beshta mudofaa qatlamining oldini olish, aniqlash, defikatsiya qilish, qarshi choralar va qayta tiklash boʻyicha xavfsizlik yechimlari ishlab chiqilishi kerak . Kelgusi 5 yil davomida avtomobilga hujumlarning oldini olish va aniqlash boʻyicha yechimlar asosiy e'tibor boʻlishi kerak, deb hisoblaymiz. Buzgʻunchilarning notoʻgʻri ma'lumotlarni yuborishi yoki avtomobildagi xizmatlarga kirishining oldini olish uchun tegishli autentifikatsiya mexanizmlarini ta'minlash juda muhimdir . Bundan tashqari, faqat vakolatli shaxslarga ruxsat berish uchun simsiz shlyuzda xavfsizlik devori koʻrinishidagi kirishni boshqarish kerak. Aniqlash avtomobilga qilingan hujumlarni aniqlash uchun zarurdir va simsiz shlyuzga roʻyxatga olish yordam dasturi va hujumni aniqlash tizimi kiritilishi kerak.

Kelgusi 10 yil ichida biz avtomobil ichidagi tarmoqdagi hujumlarning oldini olish va aniqlash muhum ahamiyatga ega ekanligini koʻramiz. Bundan tashqari, avtomobil ichidagi tarmoqdagi hujumlarni buzish va ularga qarshi choralar koʻrish uchun echimlar koʻrib chiqilishi kerak. Avtomobil ichidagi tarmoqdagi ECU oʻrtasidagi aloqada ma'lumotlarni autentifikatsiya qilish tajovuzkorlar ma'lumotlarni kiritish va oʻzgartirishni oldini olish uchun zarur. Bundan tashqari, real vaqt rejimida cheklangan avtomashina tarmogʻidagi hujumlarni aniqlash uchun roʻyxatga olish va aniqlashning engil va koʻzga tashlanmaydigan mexanizmi talab qilinadi . Bundan tashqari, ruxsatsiz kirish urinishlari va ECUga kirishga urinishlar maxsus aniqlash va qayd etish orqali aniqlanishi va qayd etilishi kerak. Avtotransport tarmogʻida roʻyxatga olish jarayoni. Avtomobil ichidagi tarmoqqa qilingan hujumlarni yaxshiroq tushunish uchun, honeypotlar kabi defiksion tizimlarni qoʻllash kerak. Honeypotsning maqsadi xavfsizlik echimlarini keyingi tadqiq qilish uchun foydali boʻlgan hujum harakati va hujum usullari haqida ma'lumot toʻplashdir. Bundan tashqari, avtomobil ichidagi tarmoqdagi faol hujumlarga qarshi turish uchun tegishli qarshi himoya mexanizmlarini oʻrganish kerak. Oldini olish va aniqlash asosan passiv himoya mexanizmlari

bo‘lib, avtomobil ichidagi tarmoqdagi faol hujumlarning oldini olish uchun faol kirishni oldini olish tizimi zarur.

Keyingi 20 yil davomida biz xavfsizlik bo‘yicha qat'iy echimlar ishlab chiqilgan va transport vositalarida joylashtirilganiga ishonamiz. Biroq, transport vositalariga kiberhujum qilish urinishlari, ehtimol, davom etadi va yanada rivojlangan bo‘ladi, chunki tajovuzkorlar himoya mexanizmlari haqida ko‘proq bilib oladilar va rivojlanadi. Shuning uchun tadqiqotning asosiy e'tibori bunday hujumlarni tiklashga qaratilishi kerak. Hujum sababini aniqlash va hujum oqibatlarini kuzatish uchun avtomobil ichidagi tarmoqda tegishli ma'lumotlar saqlanishi kerak. Kiberhujumlar halokatli oqibatlarga olib kelishi mumkin va ularni og‘ir jinoyatlar deb hisoblash kerak. Huquqni muhofaza qilish organlariga ushbu jinoyatlarni tergov qilishda yordam berish uchun avtotransport tarmog‘ida raqamli sud-ekspertiza o‘tkazish uchun echimlar ishlab chiqilishi kerak. Kiber jinoyatchilarni kuzatish va kuzatish uchun zarur ma'lumotlar tarmoqda mavjud bo‘lishi kerak. Bundan tashqari, transport vositalari bilan bog‘liq jismoniy va raqamli jinoyatlar bo‘yicha sud-tibbiy tekshiruvni o‘tkazish tartib-qoidalarini ishlab chiqish kerak.

Avtomobil kiberfizik tizimlarining yaqinlashib kelayotgan tendentsiyasi xavfsizlikka oid bir qator muammolarni keltirib chiqaradi . Avtomobil sanoati an'anaviy ravishda asosan xavfsizlik masalalari bilan shug‘ullanadi va shuning uchun transport vositalarining kelajakdagi xavfsizlik ehtiyojlarini qondirish juda qiyin vazifadir. Avtomobil sanoati uchun aroadmap chuqur mudofaa yondashuviga amal qilishdir. Avtotransport vositalarini kiberhujumlardan himoya qilishda jiddiy muammolar mavjud va xavfsizlik yechimlarini loyihalash va tatbiq etish resurslar cheklangan ECU va avtomobil ichidagi tarmoqdagi real vaqt cheklovlarini diqqat bilan hisobga olgan holda amalga oshirilishi kerak.

FOYDALANILGANADABIYOTLAR:

1.Рахимджон, Х. (2022). 6 Новых языков программирования, которые стоит изучить. Academicia Globe: Межнаучные исследования, 3 (04), 126–135 стр.

2.Аюпов Р.Х., Кабулов А.В. Криптография и криптовалюты. Т: УзМУ имени М.Улугбека, 2008-144 стр.

3.Р.ХолдарбоевР.Абдувахобова. Кибербезопасност «Science and Education» Scientific Journal, July 2022

4.Миркомилов, Д., & Гайбуллаев, Д. (2023). Области применения технологии VR (Виртуальная реальность). Research and implementation.

5.Muxtarov, F., & Sadirova, X. (2023). Korxonada axborot xavfsizligini ta’minlashning zamonaviy usullari. Engineering problems and innovations.

6. Zokirov, S. I., Sobirov, M. N., Tursunov, H. K., & Sobirov, M. M. (2019). Development of a hybrid model of a thermophotogenerator and an empirical analysis of the dependence of the efficiency of a photocell on temperature. Journal of Tashkent Institute of Railway Engineers, 15(3), 49-57.

7.Muxtarov, F., Turdimatov, M., & Mominova, M. (2023). Umumiy o’rta ta’limga kiberxavfsizlik fanini tizimli isloh qilishning ustuvor yo ‘nalishlari. Engineering problems and innovations.

8.Muxtarov, F., Umarov, A., & Ro’zaliyev, A. (2023). Axborot tizimlarida xavfsizlik tahdidlarining tasnifi. Engineering problems and innovations.