automotive news
Kiadta a Smarter Média Kommunikációs Ügynökség (https://news.smartermedia.hu)

Pasta és ramen, avagy digitális ínyencségek a Toyota informatikai étlapján

Évről évre különleges versenyt szervez informatikahallgatók számára a Toyota. A három földrészen zajló vetélkedés célja, hogy megtalálják a legkiválóbb autóhekkereket.

Az autóiparban az év szava lehetne a SDV, azaz a szoftveralapú jármű. Habár a fogalom pontos jelentéséről megoszlanak a vélemények, az alapvető értelmezés egyértelmű: azt a járművet tekintjük szoftveralapúnak (szoftver által definiáltnak), amelynek a képességei és szolgáltatásai tetszőlegesen átprogramozhatók. A vezeték nélküli szoftverfrissítés (over-the-air) mára elterjedt gyakorlattá vált, ám egyelőre többnyire csak apróságok módosíthatók ezen a módon – új grafikát tölthetünk le az infotainment rendszerbe, finomíthatjuk a klímaberendezés működését és így tovább. A jövőben azonban a főrendszerek – a kormánymű, a futómű, a fékek, a hajtáslánc, az akkumulátor – működése is alapjaiban lesz befolyásolható ezen a módon. Erre már most is láthatunk példákat egyes gyártóknál, néhány éven belül azonban várhatóan általánossá válik, hogy szoftveres frissítések letöltésével folyamatosan optimális állapotban tarthatjuk a fedélzeti rendszerek tudását.

Ez, valamint az OTA frissítésekhez elengedhetetlen internetes kapcsolat ugyanakkor rendkívül sérülékennyé teszi az autókat: bárki megpróbálhat programokat feltölteni mások járművébe, amelyekkel aztán átvehetik az irányítást az autó felett. Annak fényében, hogy az átlagember mennyire nincsen tudatában a kiberbűnözés veszélyének, és olykor komoly nagyvállalatok is hekkertámadás áldozatául esnek, belátható, hogy a védekezést nem lehet, nem szabad a felhasználóra bízni: azt az autógyártóknak kell megoldaniuk.

A Toyota évente megrendezett hekkerversenye, a Hack Festa pont ezt a célt szolgálja. Japánban, az Egyesült Államokban és Írországban gyűlnek össze informatikával foglalkozó fiatalok, hogy négyes csoportokat alkotva igyekezzenek minél frappánsabb megoldásokat találni a Toyota által kiadott feladatokra. Megpróbálják befolyásolni egy autó motorjának a fordulatszámát, módosítani a tempomat beállításait, vagy letiltani az ügyfél hozzáférését az autóhoz – az alábbi videón arra láthatunk példát, amikor egy hekkerek által írt programsor átveszi az irányítást az elektronikus (steer-by-wire) kormánymű felett.

VIDEO: https://youtu.be/pUj56fbQMnE

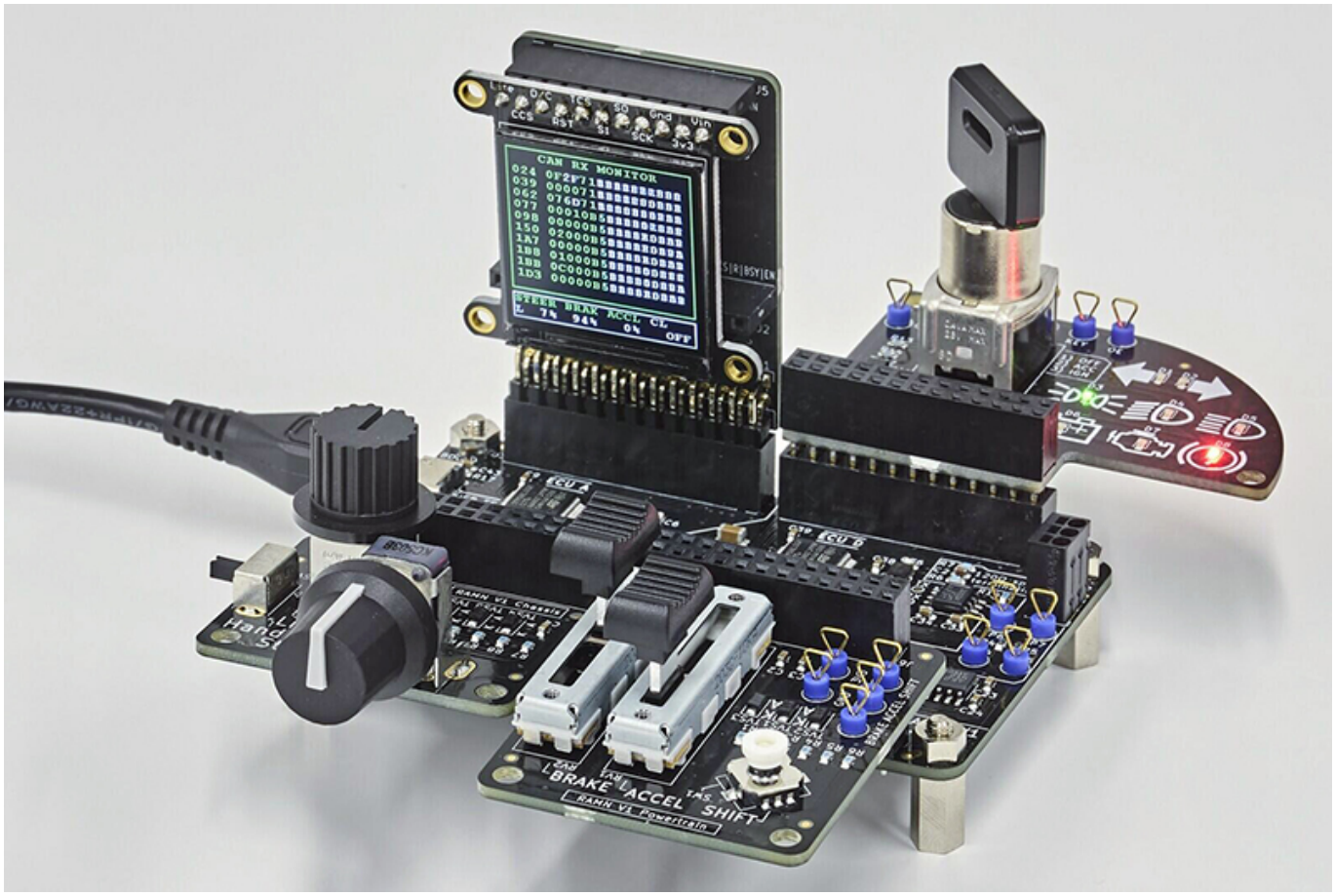
A megoldások hatékonyságát és kivédhetőségét egyaránt pontozzák, így az a csapat lesz a győztes, aki a leghatékonyabb támadást fejlesztette ki. A vetélkedés olykor euforikus hangulatban zajlik, a diákok és a támogatásukra kirendelt mentorok egy emberként örülnek, ha sikerül elegáns megoldást adni egy feladatra.

Felmerülhet a kérdés: miért jó fiatalokat arra biztatni, hogy törjék fel autók elektronikus

rendszerét? A válasz egyszerű: ugyanazért, amiért a bankok, biztosítótársaságok és egyéb, érzékeny adatokat vagy kritikus vezérlő feladatokat kezelő szervezetek hasonló próbatámadásokat szerveznek saját rendszereik ellen. Így lehet ugyanis kifejleszteni a leghatékonyabb védelmi megoldásokat – azok a fiatalok pedig, akik részt vesznek a Toyota Hack Festán, talán pont itt kapnak kedvet ahhoz, hogy később az autóiparban helyezkedjenek el kiberbiztonsági szakemberként. Ez a terület (mármint a szoftveralapú járművek műfaja) ugyanis annyira új, hogy sokan nem is tudnak a létezéséről.

Megszokhattuk persze a Toyotától, hogy egy problémára igyekszik minél több választ adni – kiváló példa erre az a multi-energia-szemlélet, amivel minden elképzelhető üzemanyagtípust igyekeznek bevonni a károsanyag-kibocsátás elleni küzdelembe, az ügyfelekre bízva a végső döntést, hogy melyik hajtásláncopciót választják.

Ezért amellett, hogy évente több tucat diák szakmai fejlődéséhez járul hozzá, a cég mérnökei építettek egy szimulátort, amely a PASTA nevet kapta. Ennek természetesen semmi köze az olasz tésztához: a név a Portable Automotive Security Testbed with Adaptability (magyarul hordozható, alkalmazkodó autóipari biztonsági tesztkészülék) kifejezés betűszava. A Toyota a modern autók összes vezérlő szoftverét belezsúfolta egy apró bőröndbe, amivel a hekkerek számítógépére csatlakoztatva teljesen valósághűen tesztelhető minden járműfunkció, anélkül, hogy a laboratóriumba be kellene vinni egy autót. Az élethűbb szimuláció érdekében a számítógépes kormánykerék és pedálok is csatlakoztathatók a berendezésbe, ám azok nélkül is tökéletesen alkalmas a feladata ellátására.



Mivel pedig a kiberbiztonság nem csak a Toyotát fenyegető kockázat, a cég nyílt forráskódú rendszerként tervezte meg a PASTA-t, így azt az egyetemektől kezdve a beszállítókig bárki továbbfejlesztheti, saját igényeihez igazíthatja, lehetővé téve a széles körű,

költséghatékony kutatást, fejlesztést és tanulást. A PASTA-bőrönd szabadon megvásárolható, méghozzá önköltségi áron, hogy minél többen hozzájuthassanak ehhez az eszközhöz, és elkezdődhessen egy világméretű együttműködés az autóipari kiberbiztonság területén.

Így is lesznek persze, akik érdeklődnek a téma iránt, ám nem engedhetik meg maguknak a PASTA beszerzését. A Toyota ezért megtervezte a rámentt – pontosabban a RAMN-t (Resistant Automotive Miniature Network, rezisztens autóipari miniatűr hálózat), amelynek a tudása ugyan korlátozott, viszont a kereskedelemben szabadon kapható nyomtatott áramkörökből és egyéb elektronikus eszközökből bárki otthon megépítheti. A RAMN tervei és az építési útmutató ingyen letölthető az internetről, így aki rendelkezik az ehhez szükséges képességekkel, megépítheti saját autóipari hekkervédelmi tesztkészülékét.

Ezzel persze távolról sincs megoldva az autók elleni kibertámadások problémája, a Toyota azonban úgy véli, minél többen, minél több irányból közelítünk egy feladathoz, annál sokoldalúbb és megbízhatóbb megoldást találhatunk arra.

Fotók: *Toyota Times, YouTube*

Forrás:
https://news.smartermedia.hu/innovacio/pasta-es-ramen-avagy-digitalis-inyencsegek-a-toyota-informatikai-etlapjan