OBD SHIELD

A gépjárművek elektronikai rendszere sebezhető. A gyártók nem fordítanak elegendő figyelmet az autók elektronikai rendszerei komponenseinek védelmére. Az utóbbi két évtizedben a járművek diagnosztikai csatlakozói szabadon hozzáférhetőek bárki számára. Emiatt – napjaink gépjárműveinek computerizált vezérlőrendszerei – sebezhetőek, sőt az autó használata egy esetleges illetéktelen beavatkozás következményeképpen akár életveszélyes is lehet, hiszen a diagnosztikai porton keresztül egyes modellek számítógépes rendszerelemei teljesen vagy részlegesen vezérelhetővé válnak. Hivatalos források becslései alapján az EU-ban a gépjárművek több mint 80%-át a gépjárművek diagnosztikai csatlakozója sebezhetőségét kihasználva tulajdonítják el. A tolvajok egy előre felprogramozott vagy helyben felkonfigurált diagnosztikai eszköz rácsatlakoztatásával kommunikálnak közvetlenül a fedélzeti számítógéppel, illetve kerülik meg a gyári beépített immobilizer védelmét.

A fedélzeti diagnosztikai rendszer:

1996-tól az On-Board-Diagnostics-II (a továbbiakban: „OBD" vagy „OBD-II") szabvány bevezetésével a hagyományos közúti járművek egy kommunikációs standardot követnek. A jármű számítógépes egységei és a szerviz technikus által használt diagnosztikai eszköz közötti kommunikációs jel protokollja és az ú.n. OBD csatlakozó (max. 16 pin-es csatlakozó) is szabványosítva lett. Ugyanakkor a gyártók továbbra sem védték le az egyes perifériákat illetéktelen használók ellen. Ezen perifériák legjelentősebbike az OBD (diagnosztikai) port.

Az „OBD Shield" – ami egy gépjármű-biztonsági rendszer – az OBD porton tátongó biztonsági rést fedi le. A rendszer egy beépülő titkosító modulból és egy feloldó eszközből áll, amely a klasszikus man-in-the-middle támadások fordított elvén egy beépülő védelmi rendszert alkot, amely a védendő rendszer és a külső hozzáférők közé állva, blokkolja az illetéktelen hozzáférési próbálkozásokat.

Az OBD Shield működése:

A beépített védelmi áramkör – a gyári OBD csatlakozó és a védett csatlakozó között elhelyezve - egy egyedileg programozott mikrovezérlő segítségével gátolja a kommunikációt. A gépjárműben hozzáférhető OBD csatlakozó a laikus szemlélő számára eredeti, gyári alapállapotúnak (standard female OBD) tűnik, ugyanakkor a védelmi áramkör 12V-os táp vezetéken kívül semmilyen egyéb áramkört/vezetéket nem enged keresztül.

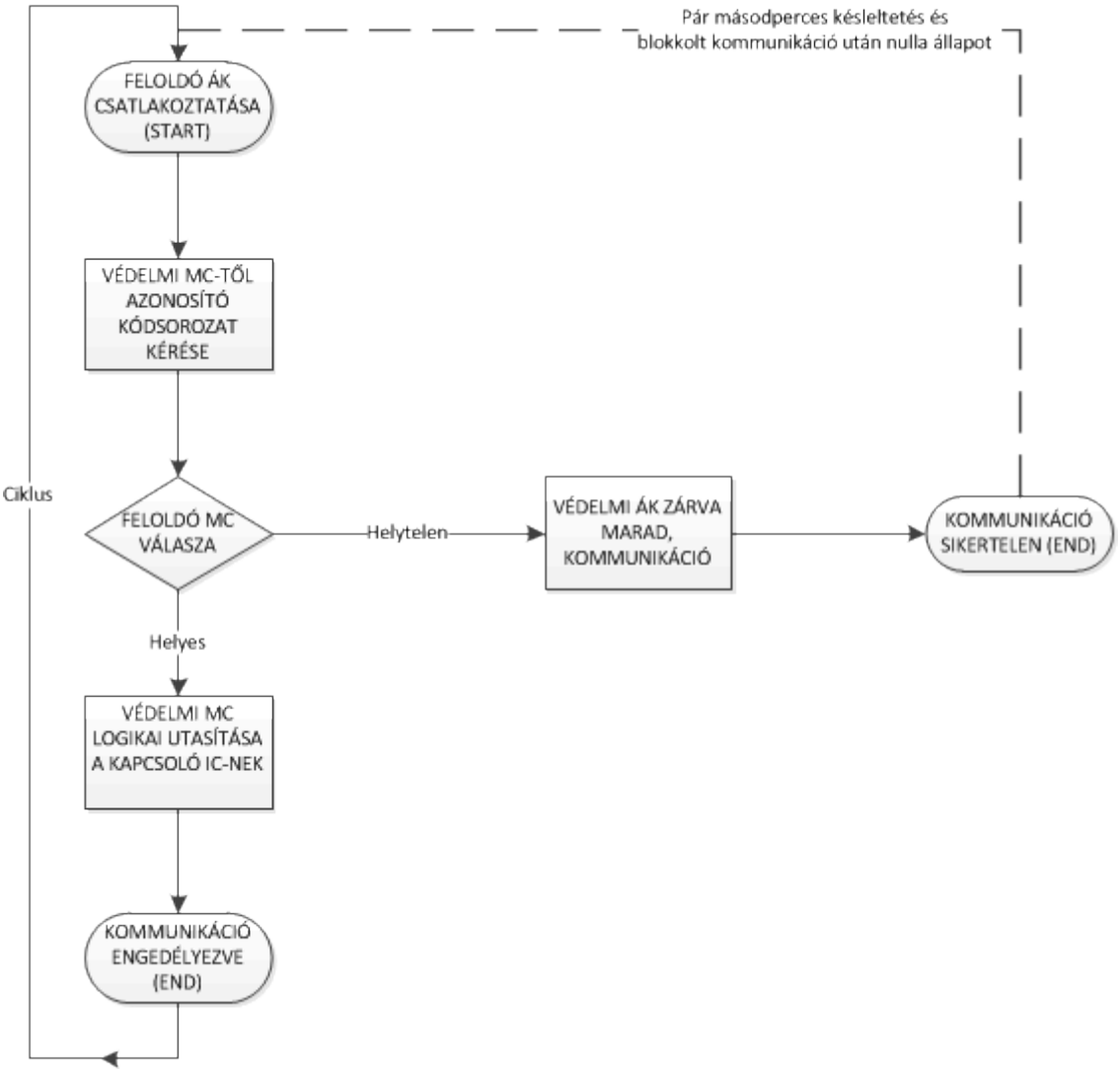
A feloldás egy szintén egyedi – a védelmi áramkör mikrovezérlőben futtatott szoftverére hangolt – áramkör végzi. A csatlakozáskor a védelmi és a feloldó eszköz mikrovezérlői egy komplex **authentikációs folyamat**ba kezdenek, amit a csatlakoztatás idejére folyamatosan fenntartanak. A diagnosztikai porton folyó kommunikáció az ellenkező feloldó ellendarab csatlakoztatása nélkül nem lehetséges.

Az authentikációs eljárás:

A védelmi és a feloldó áramköri egységek saját, egyedi kódokkal hitelesítenek. Az eredeti kód soha nem kerül átküldésre, ehelyett a rendszer véletlenszerű sorozatban komplex matematikai és logikai műveleteket végez a másodperc törtrésze alatt és ennek eredménye kerül egyeztetésre a csatlakoztatás ideje alatt ciklikusan. Amennyiben a védelmi áramkör mikrovezérlője kiküldött kérdésére a feloldó eszköz mikrovezérlőjétől helyes kódsorozatot kap, úgy a védelmi áramkör mikrovezérlője utasítást ad egy logikai IC elem számára, hogy zárja kapuit, ilyenformán az összezárja az – OBD csatlakozón végül tüskékben végződő – egyes áramköröket. Helytelen/hibás authentikáció esetén a védelmi áramkör észleli a rossz kódot vagy annak hiányát és megszakítja a kommunikációt néhány másodpercre, ezzel szinte teljesen ellehetetlenítve az eszköz és az általa védett kommunikációs csatorna kompromittálhatóságát.

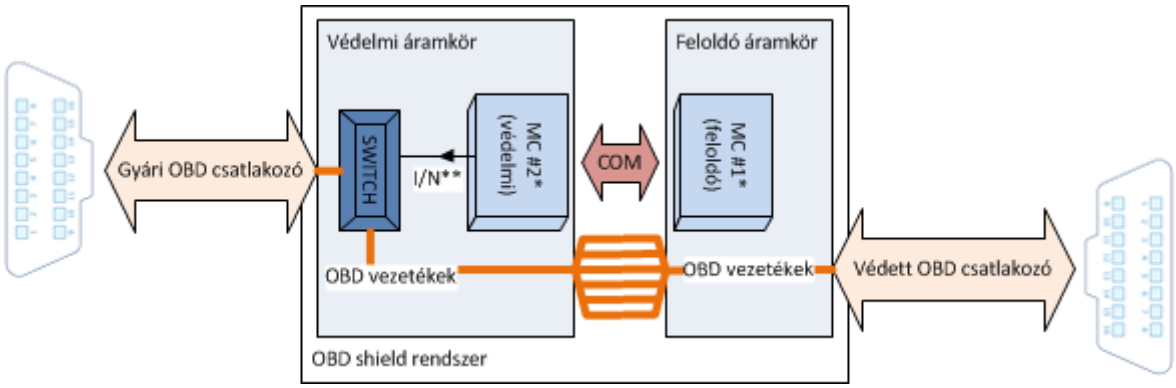
Hiába kap hozzáférést harmadik személy ideiglenesen, egyidejűleg a védelmi és a feloldó eszközhöz is egyaránt, a kommunikációs kódsorozat folyamatos változatása és a beégetett egyedi kódok miatt szinte lehetetlen az eszköz authentikációs folyamatának megfejtése.

Kommunikációs folyamatábra:



1. ábra

A rendszer blokkvázlata:



2. ábra

*MC: Mikrovezérlő
** I/N: Igen vagy Nem logikai engedélyező jel

Működés szoftveres folyamata:

Miután a Védelmi egység a gyári OBD csatlakozóra kiépítésre került, a Védelmi egység csatlakozójához csatlakoztatott Feloldó egységben található mikrovezérlő (2. ábrán az MC#1) nem ad ki jelet, mindaddig amíg nem érkezik egy véletlen authentikációs kérés az MC#2-től. Ezt az MC#1 értelmezi, majd a külső vagy belső memória modulból kinyert információ alapján, véletlenszerű logikai és matematikai műveleteket követően, kódsorozatot küld vissza ugyanazon az authentikációs eljárásra fenntartott közvetlen kommunikációs vezetéken. Az MC#2 értelmezi a jelet, majd megfejti a kódsorozatot a külső vagy belső memória moduljában tárolt információ alapján. Amennyiben az MC#1-től kapott kód helyesnek bizonyul, az MC#2-ben futó szoftver utasítást ad a mikrovezérlő egyik lábán logikai jel adására megfelelő feszültségszinten.

A jel hatására az erre a vezetékre telepített logikai kapcsoló IC elem (Switch) zárja a kapuit, ilyenformán az OBD csatlakozók felé továbbított vezetékek összezárulnak, a kommunikáció ezeken a vezetékeken engedélyezetté válik.

A mikrovezérlőkbe táplált vezérlőszoftver ciklikusan fut, azaz minden egyes sikeres authentikációt követően újrafuttatja azt, mindaddig amíg helyes kódot kap és csatlakoztatva vannak egymáshoz az egységek. Amennyiben hibás kód érkezik, vagy a Védelmi egység és a Feloldó egység szétválasztásra kerül, az MC#2-ben futó szoftver, a mikrovezérlő be-és kimenti lábait letiltja, a kommunikációt ilyenformán néhány másodpercre felfüggeszti, ezt követően újra alapállapotba áll és újra kiküldi a véletlenszerű kérést az authentikációs eljárásra fenntartott közvetlen kommunikációs vezetéken.