Fides, Ratio et Patria. Studia Toruńskie 3/2015
ISSN 2392-1463

Sławomir Jeżewski*
Wyższa Szkoła Kultury Społecznej i Medialnej w Toruniu
Wojciech Sorbian**
Centrum Techniczne Delphi, Kraków

Samochodowa sieć CAN – zagrożenia włamaniami

1. Wstęp

Współczesna motoryzacja na naszych oczach przechodzi poważną rewolucję technologiczną, podobną do tej, którą w latach siedemdziesiątych odnotowano w przemyśle lotniczym. Osią tych zmian jest odejście od elektromaszynowych systemów sterowania na rzecz sterowania mikroprocesorowego realizowanego przez wyspecjalizowane sterowniki. Sterowniki wraz z łączącą je siecią komputerową CAN (*Controller Area Network*) stanowią rozproszony system sterowania samochodem, który może być obiektem manipulacji ze strony włamywacza komputerowego. W przypadku niektórych modeli samochodów włamywacz jest w stanie tak dalece zakłócić działanie systemu sterowania, że doprowadzi do wypadku samochodowego i śmierci jego użytkownika lub/i postronnych użytkowników drogi. Może pozostawić w systemie sterowania bombę logiczną, która uaktywni się po tygodniach lub miesiącach, gdy uzna, że warunki jazdy są na tyle niebezpieczne, iż gwarantują śmiertelny skutek wypadku.

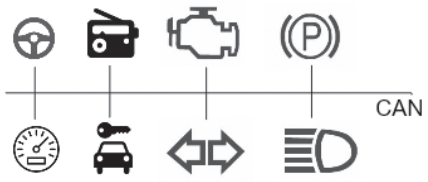
Dotychczas bezpieczeństwo sieci samochodowych nie było przedmiotem publicznej debaty, gdyż te systemy nie miały aż takiego znaczenia dla bezpieczeństwa kierowcy. Obecnie dyskusja ta wydaje się nie do uniknięcia. Co więcej, pozostawienie jej wyłącznie w gestii producentów samochodów gwarantuje, że nie zostanie ona poprowadzona należycie ze względu na ich naturalne ograniczenia dyktowane wynikiem ekonomicznym jako jedyną miarą efektywności.

* **Sławomir Jeżewski** – doktor, informatyk, pracownik naukowy Wyższej Szkoły Kultury Społecznej i Medialnej i Politechniki Łódzkiej.

** **Wojciech Sorbian** – Absolwent kierunku Elektrotechnika na Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie. W latach 2012-2014 pracownik Europejskiej Organizacji Badań Jądrowych CERN w Genewie. Aktualnie pracuje na stanowisku Inżyniera ds. Systemów w Centrum Technicznym Delphi w Krakowie zajmując się projektami związanymi z technologiami aktywnego bezpieczeństwa w samochodach.

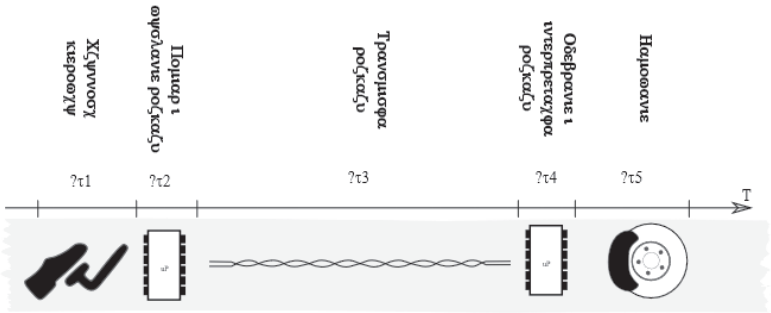
2. Idea działania współczesnego samochodu

Samochód z lat osiemdziesiątych z reguły wyposażony był w jeden sterownik elektroniczny przeznaczony do optymalizacji pracy silnika. Nie miał on wpływu na krytyczne dla bezpieczeństwa czynności sterowania samochodem, takie jak hamowanie czy zmiana kierunku jazdy. Przeniesienie akcji z „rąk" kierowcy na docelowe urządzenia było realizowane na drodze mechanicznej (cięgła i przekładnie) lub hydraulicznej. Ten styl projektowania samochodów należy uznać już za historyczny. Producenci samochodów, dążąc do redukcji kosztów, uproszczenia konstrukcji mechanicznych, zmniejszenia ilości okablowania w samochodzie i zmniejszenia jego masy, zaproponowali i wdrożyli schemat budowy samochodu oparty o sieć komputerową.



Rys. 2.1. Ideowy schemat systemu sterowania samochodem

Centralnym elementem tego systemu jest sieć komputerowa CAN łącząca poszczególne urządzenia wykonawcze samochodu. Każde urządzenie, takie jak pedał hamulca, kierownica, przełącznik świateł, jest teraz układem mikroprocesorowym wysyłającym do swoich odbiorców komunikaty.



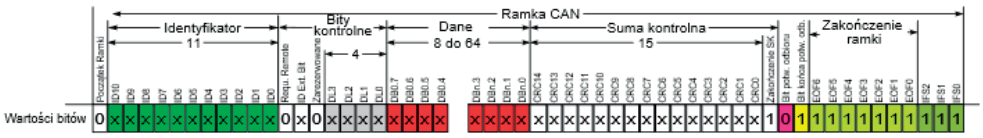
Rys. 2.2. Schemat procesu hamowania

Ideę działania takiej sieci łatwo można zrozumieć, analizując przebieg przykładowego procesu sterowania, np. hamowania (rys. 2.2). Proces hamowania przebiega w pięciu etapach. Najpierw kierowca naciska pedał hamulca. Zmiana położenia dźwigni hamulca jest wykrywana i interpretowana przez skojarzony z nim mikroprocesor. Przelicza on położenie dźwigni hamulca na siłę hamowania wyrażoną np. w procentach i wysyła tę wartość w postaci komunikatu sieciowego. Komunikat ten jest odbierany przez procesory odpowiadające za hamulce poszczególnych kół samochodu. Procesory te odbierają komunikat, interpretują go i zmieniają ciśnienie w cylindrach hamulcowych, efektywnie wywołując proces hamowania.

3. Sieć CAN i jej charakterystyka

Sieć CAN zaprojektowana została w latach siedemdziesiątych w firmie Robert Bosh GmbH przez jej twórcę [Lawrenz][Bosch GmbH]. Przy jej projektowaniu autor skupił się na zagadnieniach odporności sieci na zakłócenia elektryczne i magnetyczne. Ta właśnie odporność stała się źródłem sukcesu rynkowego sieci CAN i późniejszej standaryzacji rozwiązania. Niestety przy projektowaniu sieci i protokołu komunikacyjnego nie rozważył on odporności sieci na włamania i ataki typu DoS (*Denial of Service*), bo tego typu problemy w latach siedemdziesiątych nie istniały. Przez to wiele cech sieci CAN, uprzednio stanowiących o jej sukcesie rynkowym, obecnie jest kwestionowanych z punktu widzenia bezpieczeństwa samochodu i pasażerów.

Zgodnie z projektem CAN jest siecią równouprawnionych sterowników połączonych elektryczną magistralą transmisyjną. Sterowniki wysyłają do siebie krótkie komunikaty, w których zawarte są polecenia, wyniki pomiarów lub wyniki pośrednich obliczeń, i w ten sposób realizują zadania sterowania. Komunikat sieci CAN składa się z adresu fizycznego, identyfikatora, pól pomocniczych oraz maksymalnie ośmiu bajtów danych [ISO 11898-2:2003]. Poniższy rysunek przedstawia go szczegółowo.



Rys. 3.1. Budowa ramki CAN

Z budowy ramki CAN wynika kilka cech rzutujących na bezpieczeństwo transmisji.

3.1. Brak adresu (identyfikatora) nadawcy

W ramce CAN nie przewidziano miejsca na adres/identyfikator nadawcy. Zawarty w niej identyfikator wiadomości działa jako identyfikator typu danych przesyłanych w ramce. Każdy węzeł sieci – zarówno uprawniony, jak i nieuprawniony – ma prawo wysłać komunikat z danym identyfikatorem. W ten sposób jeden węzeł sieci może podszyć się pod inny i w jego imieniu wysłać komunikat. Także ten kluczowy dla bezpieczeństwa kierowcy.

3.2. Metoda dostępu do medium transmisyjnego nieodporna (na ataki DoS)

Sieć CAN zaprojektowana została jako sieć równoprawnych węzłów, w której każdy węzeł ma prawo rozpocząć nadawanie bez wezwania. Taka koncepcja współpracy z siecią niesie ryzyko, że dwa węzły rozpoczną nadawanie jednocześnie, przez co odbiorcy otrzymają uszkodzony komunikat. Aby tego uniknąć, należy opracować algorytm arbitrażu rządzący dostępem do medium transmisyjnego. W sieci CAN zaprojektowano go w oparciu o właściwości elektryczne sieci. Algorytm oparty jest na koncepcji „logiki na drucie" z dominującym zerem. Osią koncepcji jest spostrzeżenie, że jeśli dwa węzły nadają sygnał jednocześnie, jeden z nich nadaje stan wysoki „1", a drugi – stan niski „0" (zwarcie do masy), to linia nadawcza przyjmie stan niski „0". W ten sposób węzeł nadający, który monitoruje stan linii nadawczej, w trakcie nadawania jest w stanie zorientować się, że ktoś inny nadaje równocześnie z nim. Poniżej przedstawiono algorytm arbitrażu w postaci pseudokodu.

```
IF Trwa nadawanie THEN
    Czekaj na koniec nadawania
END IF
FOREACH bit identyfikatora wiadomości DO
    wysteruj linię CAN zgodnie z wartością bitu
    odczekaj, by napięcie na linii się ustabilizowało
    odczytaj stan linii CAN
IF stan nadawany <> stan odczytany THEN
    // ktoś inny nadaje równocześnie i nadał bit o wartości 0
    przerwij nadawanie i rozpocznij algorytm od początku
END IF
DONE
```

Rys. 3.2. Algorytm arbitrażu przy dostępie do linii nadawczej

Przedstawiony algorytm dostępu do sieci cechuje prostota i oszczędność pasma transmisyjnego. Daje on pierwszeństwo nadawania tym komunikatom, które mają niższy identyfikator. Jest on również przyczyną nieodporności na ataki DoS. Węzeł sieci opanowany przez hakera (węzeł atakujący) jest w stanie wysyłać cyklicznie komunikaty z niskim identyfikatorem (np. 0 x 0 lub 0 x 1) i w ten zablokować całą sieć. Węzeł atakujący z bardziej rozbudowanym algorytmem może uniemożliwić wysyłanie jednego lub kilku wybranych komunikatów.

3.3. Brak potwierdzeń komunikatów

Konstruując sieci samochodowe, przyjęto, że komunikaty sieci CAN nie wymagają potwierdzenia w postaci komunikatu zwrotnego. Jest to pochodna rozgłoszeniowego charakteru tych komunikatów. Tym samym przyjęto koncepcję sieci, która w warstwie transportowej jest siecią bezpołączeniową i stratną. W takiej sieci komunikaty mają prawo ginąć. Jest to sytuacja, w której komunikat został prawidłowo nadany, ale nie został odebrany przez węzeł odbiorczy. Problem z utraconymi komunikatami przesunięto do warstwy aplikacji i rozwiązano w najmniej udany sposób. Przyjęto, że jeżeli komunikaty mogą ginąć, to będą one cyklicznie aktualizowane, i to w takim tempie, by utracenie pojedynczego komunikatu nie było istotne dla całego systemu. W ten sposób we współczesnym samochodzie obciążenie sieci CAN często sięga górnej dopuszczalnej granicy 70 procent, przy czym większość transportowanych komunikatów nie niesie istotnie nowych informacji. Ten natłok cyklicznie wysyłanych komunikatów ma swoje znaczenie dla bezpieczeństwa, a w szczególności dla skutecznego szyfrowania i deszyfrowania komunikatów.

3.4. Brak szyfrowania

Większość współcześnie użytkowanych samochodów posiada sieć CAN pozbawioną szyfrowania. Powyższa uwaga dotyczy także marek samochodów powszechnie uznawanych za luksusowe (VIP) i autobusów. Producenci samochodów, którzy chcieliby zastosować skuteczne i odporne na ataki hakerów szyfrowanie w swojej sieci samochodowej, natrafią na szereg trudności:

1. Muszą uzgodnić algorytm szyfrowania z wszystkimi swoimi poddostawcami.
2. Muszą gruntownie zmienić sposób budowy komunikatu CAN, łamiąc przy tym zasady obecnie przyjętego standardu CAN 2.0 [ISO 11898-1:2003],[ISO 11898-2:2003],[ISO 11898-3:2006].
3. Muszą zaakceptować wyższe koszty instalacji elektrycznej i wyższe zużycie energii przez te układy ze względu na szyfrowanie.

4. Muszą zastosować wyższe częstotliwości transmisji danych na linii komunikacyjnej, tak by szyfrowanie danych nie doprowadziło do przeciążenia sieci.

Komponenty samochodowego systemu sterowania rzadko kiedy wytwarzane są w całości przez producenta samochodów. Wiele komponentów zleca się do wykonania kooperantom i im należałoby przekazać szczegóły algorytmu szyfrowania, by mogli go zaimplementować w swoich rozwiązaniach. W takich warunkach trudno mówić o poufności takiego algorytmu, co wymusza stosowanie bardziej złożonych obliczeniowo algorytmów.

Najistotniejsza z punktu widzenia włamującego się hakera informacja to identyfikatory komunikatów. One pozwalają na rozróżnienie i wychwycenie tych komunikatów, które mają znaczenie krytyczne dla bezpieczeństwa (uruchomienie hamulców). Przy obecnej budowie komunikatów sieci CAN nie mogą być zaszyfrowane, bowiem stanowią one element arbitrażu przy dostępie do medium transmisyjnego. Aby można było szyfrować identyfikatory komunikatów, należałoby zmodyfikować gruntownie standard CAN. Szyfrowanie znacznie obciąża procesory poszczególnych węzłów, przez co rośnie koszt węzłów sieci i całkowity koszt instalacji elektrycznej. W zaszyfrowanej sieci każdy komunikat sieciowy musiałby zostać rozszyfrowany przez dany węzeł, by mógł się on dowiedzieć, czy komunikat jest do niego. Autorzy pomijają w tych rozważaniach procesory ze sprzętowo zaimplementowanym algorytmem szyfrowania ze względu na ich oczywistą bezużyteczność.

Algorytm szyfrowania, aby był skuteczny, musi wydłużyć komunikat. W ten sposób zwiększona zostanie entropia komunikatu i trudniejsze będzie złamanie szyfru. W obecnie stosowanym standardzie CAN długość komunikatów nie podlega negocjacji i wynosi czternaście bajtów (osiem bajtów danych + identyfikator i dane kontrolne). Nawet nieznaczne zwiększenie długości komunikatu może zaowocować dwukrotnym czy trzykrotnym zwiększeniem obciążenia sieci (dwie ramki zamiast jednej).

Podsumowując rozważania dotyczące szyfrowania komunikatów w sieci CAN, należałoby stwierdzić, że obecny standard sieci CAN nie jest przystosowany do szyfrowania komunikatów i wręcz utrudnia stosowanie takiego szyfrowania.

4. Sposoby włamania do samochodowego systemu informatycznego

W niniejszym rozdziale autorzy scharakteryzują trzy podstawowe sposoby włamania do systemu informatycznego samochodu:

1. Atak przez fizyczne dołączenie urządzenia do magistrali samochodowej.

2. Atak poprzez zmianę oprogramowania jednego z istniejących urządzeń mikroprocesorowych w samochodzie.
3. Atak poprzez komputer multimedialny podłączony do Internetu.

W swoich rozważaniach autorzy przyjmują, że celem hakera jest morderstwo przeprowadzone w taki sposób, by zaistniała sytuacja była niemożliwa do odróżnienia od wypadku samochodowego.

4.1. Atak poprzez fizyczne dołączenie urządzenia do magistrali

Najłatwiejszym, a jednocześnie najbardziej brzemiennym w skutki sposobem ataku jest wpięcie dodatkowego urządzenia w magistralę CAN [Illera, Vidal]. Haker może podejść do zaparkowanego samochodu i bez jego otwierania dopiąć do niego swoje własne urządzenie. System informatyczny współczesnego samochodu nie jest w stanie wykryć dodatkowego urządzenia na linii CAN. Urządzenie takie może monitorować prędkość samochodu, konfigurację drogi (zakręty), a w niektórych samochodach także obecność obiektów na drodze (samochodów, motocykli) oraz obiektów w pasie przydrogowym. Węzeł hakera może uaktywnić się, gdy warunki otoczenia wskazują na niebezpieczną sytuację, i zmodyfikować akcje sterowania ze strony kierowcy tak, by wywołać wypadek. Może zakłócić sterowanie siłą hamowania poszczególnych kół lub sterowanie prędkością jazdy. W polskiej praktyce dochodzeniowej nie poddaje się powypadkowego samochodu drobiazgowej kontroli, więc tego typu wypadek zostałby zakwalifikowany jako błąd kierowcy i utrata kontroli nad samochodem lub niezachowanie bezpiecznej prędkości jazdy. Jednakże haker pozostawia po sobie ślad w postaci dodatkowego urządzenia, które mogłoby zostać odkryte w trakcie szczegółowego badania technicznego.

Lepiej wykwalifikowany i dysponujący większymi środkami haker mógłby wymienić jedno z urządzeń podłączonych do sieci CAN na swoje własne, realizujące wszystkie czynności oryginalnego urządzenia oraz dodatkowe funkcje zlecone przez hakera. Takim urządzeniem mogą być: lampy kierunkowskazów, reflektory przednie i lampy tylne, sygnał dźwiękowy czy generalnie wszystkie urządzenia o stosunkowo prostej funkcjonalności dostępne z zewnątrz samochodu bez jego otwierania.

Tak zmodyfikowane urządzenie przejdzie najbardziej drobiazgową kontrolę powypadkową, nie budząc podejrzeń. Obecnie nie ma technicznego sposobu na inspekcję oprogramowania zawartego w takim urządzeniu i porównanie go z fabrycznym oryginałem. Nawet jeśli urządzenie oferuje możliwość odczytania oprogramowania przez magistralę CAN, to cały ten proces realizowany jest przez działające w urządzeniu oprogramowanie, czyli oprogramowanie, którego autentyczność kwestionujemy.

4.2. Atak poprzez zmianę oprogramowania jednego z węzłów sieci

Większość urządzeń mikroprocesorowych we współczesnym samochodzie realizuje złożone lub bardzo złożone funkcje. Mimo dużego wysiłku wkładanego w niezawodność oprogramowania tych urządzeń producenci nie są w stanie zagwarantować jego bezawaryjności. Zwykle zostawiają sobie możliwość aktualizacji oprogramowania w celu usunięcia błędów znalezionych podczas eksploatacji. Aktualizacji oprogramowania dokonuje się w stacji diagnostycznej w trakcie przeglądu przy użyciu specjalistycznego oprogramowania diagnostycznego. Mechanizm aktualizacji oprogramowania jest idealnym punktem ataku dla hakera. Jest jednocześnie punktem wyjścia do dyskusji na temat roli stacji obsługi pojazdów i warsztatów w zapewnieniu bezpieczeństwa pasażerów. Problem ten nabiera szczególnej ostrości w przypadku samochodów rządu RP, samochodów działaczy politycznych oraz wysoko postawionych ludzi biznesu. Mechanizm aktualizacji oprogramowania zawiera cały szereg luk, poczynając od systemu uwierzytelnienia swoistego dla całej rodziny samochodów, a kończąc na zbyt krótkich kluczach i hasłach.

4.3. Atak poprzez komputer multimedialny

Kokpit współczesnego samochodu oferuje wiele funkcji związanych z odtwarzaniem muzyki, słuchaniem radia, współpracą z telefonami komórkowymi, aktywnym pobieraniem danych z Internetu. Zadania te realizowane są przez dedykowany komputer, zwany komputerem multimedialnym. Bardzo często komputer ten połączony jest na stałe z Internetem i posiada swój własny numer IP, a jego oprogramowanie zbudowane jest na bazie typowego systemu operacyjnego (Linux, QNX itp.).

Te dwie informacje wystarczają hakerom do przeprowadzenia ataku na komputer multimedialny i uzyskania praw administratora. Poprzez uzyskanie tych praw haker umożliwia sobie uruchomienie dowolnego programu, także tego wytworzonego samodzielnie. Jeśli komputer multimedialny podłączony jest do głównej magistrali CAN samochodu, haker uzyskuje wpływ na działanie samochodu tak samo skutecznie, jakby podłączył swój własny węzeł sieci. Ten typ ataku wymaga relatywnie dużej wiedzy na temat włamań do systemów informatycznych, ale można tu stosować klasyczne techniki włamań do serwerów internetowych.

Producent samochodu może w łatwy sposób ograniczyć rozległość takiego ataku poprzez odizolowanie komputera multimedialnego od głównej magistrali CAN filtrem pakietów (*gateway*).

5. Koncepcja ochrony przed atakami

Przedstawione sposoby włamania do sieci komputerowych należy przeanalizować w kontekście tego, kto jest celem ataku i w jakim miejscu ma on być przeprowadzony. Autorzy osobno rozważą bezpieczeństwo anonimowego obywatela, osób biorących aktywny udział w polityce lub zarządzających przedsiębiorstwami o zasięgu krajowym i zagranicznym, Prezydenta i Rządu RP, samochodów i pojazdów używanych przez Wojsko Polskie (WP).

Takie rozgraniczenie ma sens ze względu na większy lub mniejszy dostęp atakującego do wysokich technologii, wysoko wykwalifikowanych specjalistów, funduszy i czasu.

Cel ataku (typ pojazdu) / **Miejsce ataku**	**Obywatel (samochód seryjny)**	**VIP (samochód seryjny konfigurowany na żądanie)**	**Rząd RP (samochód specjalny)**	**WP (samochód specjalny)**
Fabryka producenta samochodu lub jego poddostawcy	Brak zagrożenia	Średnie zagrożenie	Wysokie zagrożenie	Wysokie zagrożenie
Warsztat naprawczy, serwis	Średnie zagrożenie	Wysokie zagrożenie	Wysokie zagrożenie	Niskie zagrożenie
Miejsce parkowania	Wysokie zagrożenie	Wysokie zagrożenie	Niskie zagrożenie (samochód nadzorowany w trakcie postojów)	Brak zagrożenia
Atak poprzez komputer multimedialny	Wysokie zagrożenie	Wysokie zagrożenie	Wysokie zagrożenie (standardowe seryjne systemy multimedialne)	Brak zagrożenia, brak standardowych połączeń do sieci

5.1. Ochrona obywatela

Najpoważniejszym zagrożeniem dla szeregowego obywatela jest dołączenie przez hakera dodatkowego węzła do magistrali CAN lub podmiana jednego z dostępnych zewnętrznie urządzeń. Jedynym sposobem ochrony przed tego typu atakiem jest zmiana standardu sieci CAN pozwalająca na zaszyfrowanie komunikatów. Algorytm szyfrowania powinien być oparty o klucze unikalne dla danego samochodu, nie zaś rodziny samochodów. Złożoność pamięciowa algorytmu deszyfracji powinna być nie mniejsza niż 1 GB, zaś złożoność czasowa nie mniejsza niż 5 lat. Zaszyfrowana wiadomość powinna zawierać dane uwierzytelniające co najmniej takie, jak podpis elektroniczny węzła wysyłającego i stempel czasowy.

Algorytm szyfrowania danych transmitowanych po sieci nie zabezpieczy użytkownika samochodu przed manipulacją w warsztacie samochodowym. Działania naprawcze i diagnostyczne wymagają dostępu do sieci CAN, a więc i do kluczy szyfrowania. Jeśli wynikiem działań serwisu będzie aktualizacja oprogramowania, to właściciel samochodu nie będzie w stanie ocenić zasadności tego działania ani jego poprawności.

Do ochrony właściciela samochodu potrzebne jest dodatkowe urządzenie odpowiadające funkcjonalnie czarnej skrzynce samolotu. Urządzenie to miałoby za zadanie przechowywać wszystkie wiadomości CAN przesyłane na magistrali CAN w ciągu ostatnich 24 godzin. Prócz tego czarna skrzynka musiałaby przechowywać ślad istotnych działań diagnostycznych, takich jak zmiana oprogramowania, zmiana parametrów kalibracyjnych itp. Zapis czarnej skrzynki byłby podstawą analizy sytuacji w trakcie wypadku i wykluczenia celowej manipulacji samochodem w celu wywołania wypadku.

Aby koncepcja czarnej skrzynki była skuteczna, potrzebne jest wprowadzenie norm legislacyjnych i narzucenie firmom samochodowym obowiązku przygotowania samochodu do instalacji skrzynek. Ponadto wskazane jest wprowadzenie dodatkowych uregulowań zapobiegających monopolizacji rynku:

Właścicielem projektu czarnej skrzynki: koncepcji, dokumentacji mechanicznej, dokumentacji elektronicznej oraz jej oprogramowania, powinna być agenda rządowa, np. Komenda Główna Policji.

Agenda rządowa nie miałaby prawa produkować czarnych skrzynek samodzielnie, za to projekt ten powinien być dzierżawiony przedsiębiorstwom, podmiotom gospodarczym w zasadzie bez opłat.

Proces produkcji czarnych skrzynek powinien podlegać atestowaniu i cyklicznej kontroli ze strony agendy rządowej.

5.2. Ochrona Rządu RP i Prezydenta

Samochody rządowe należą do kategorii samochodów specjalnych. Są zamawiane i produkowane w trybie indywidualnym. W obecnej rzeczywistości ekonomicznej są to wyłącznie samochody produkowane poza granicami kraju. Jednym z elementów kontraktu na samochód rządowy powinno być pozyskanie kodu źródłowego oprogramowania wszystkich elementów sieci CAN. Jeśli producent nie chce (nie może) przekazać kodu źródłowego oprogramowania, musi zgodzić się na ekspertyzę oprogramowania przeprowadzoną przez polskich specjalistów w ich siedzibie. Jeśli producent nie chce spełnić nawet tego warunku, jego oferta powinna być bezwzględnie odrzucona. Większość węzłów sieci CAN, z wyjątkiem komputera głównego (*body computer*), posiada niezbyt rozbudowane oprogramowanie (mniej niż około 100 tysięcy linii kodu). Ekspertyza kodu źródłowego jest

możliwa do wykonania i zabezpiecza przeciwko atakowi hakerskiemu przeprowadzonemu w siedzibie producenta samochodu. Atak w warsztacie naprawczym czy w trakcie parkowania autorzy uznają za mało prawdopodobny ze względu na stały nadzór nad samochodem ze strony warsztatu i ochrony rządowej.

5.3. Ochrona osób odgrywających istotne role społeczne (VIP)

Właściciele przedsiębiorstw, politycy, naukowcy, dziennikarze to osoby, które mogą odgrywać istotną rolę społeczną. Mogą być obiektem zainteresowania lub ataku ze strony osób, organizacji lub służb wywiadowczych spoza granic RP. Osoby takie zwykle nie posiadają wiedzy z zakresu techniki samochodowej wystarczającej do rozpoznania tego typu zagrożeń, ani też środków technicznych do skutecznej ochrony przed nimi. Spośród wyróżnionych grup użytkowników samochodów są to osoby najbardziej narażone na skuteczny atak. Do ochrony takich osób wymagane byłoby:

Wprowadzenie szyfrowania wiadomości wysyłanych siecią CAN w oparciu o klucze indywidualne dla egzemplarza samochodu.

Wprowadzenie kluczy deszyfrujących na dwu poziomach. Klucze poziomu pierwszego odszyfrowują wiadomości CAN. Klucze poziomu drugiego uprawniają do uaktualniania oprogramowania. Klucze poziomu drugiego są w wyłącznym posiadaniu właściciela samochodu i mają formę karty mikroprocesorowej.

Wprowadzenie czarnej skrzynki zgodnie z uprzednim opisem.

5.4. Ochrona samochodów wojskowych

Stosunkowo najprościej opisać zasady ochrony samochodów wojskowych. W przypadku takich pojazdów wymagane jest przekazanie Wojsku Polskiemu kodu źródłowego wszystkich węzłów sieci CAN i praw do uaktualniania oprogramowania. Niestety nawet takie zabezpieczenie nie uchroni samochodów wojskowych przed ingerencją z zewnątrz, bowiem manipulacje mogą być zawarte w silikonie procesorów użytych do budowy systemów mikroprocesorowych (np. technologia VPRO). Samochody i sprzęt wojskowy nie mogą być uważane za zabezpieczone przed atakami, jak długo używane w nich będą procesory produkowane poza granicami kraju.

6. Podsumowanie

W niniejszym artykule przedstawiono trzy podstawowe sposoby włamania do samochodowej sieci CAN i możliwe konsekwencje tych włamań. Wykazano, że przy obecnym stanie techniki samochodowej jest możliwe przeprowadzenie

zamachu na osobę dysponującą nowoczesnym samochodem i że zamach ten może ujść uwadze polskich służb dochodzeniowych. Wykazano również, że Rząd RP i Wojsko Polskie musi uwzględniać tę część techniki samochodowej w swoich procedurach bezpieczeństwa.

Przedstawiono dwie koncepcje ochrony obywateli polskich przed próbami morderstwa:

- szyfrowanie komunikatów na magistrali CAN,
- stosowanie czarnych skrzynek w celu wykrycia manipulacji samochodem.

Obydwie te koncepcje wymagają inicjatywy legislacyjnej ze strony Państwa Polskiego.

Słowa kluczowe: *samochodowa sieć CAN, bezpieczeństwo, ochrona, systemy mikroprocesorowe*

Summary

Automotive CAN network – hacking threats

Current vehicle designs undergo real technological revolution in recent years, similar to the one which already happened in the aerospace industry in the seventies. Reason for those changes was replacement of electromechanical control systems with microprocessor-based systems, which in turn were connected by larger control networks. Internal vehicle communication networks can become a target for hacker, who, with specialized knowledge, can influence behavior of this network and alter vehicle reactions to control inputs. One could even place "logic bomb", advanced algorithms which would wait until dangerous driving conditions are detected and only then activate itself, leading in turn to severe accidents.

So far security of car communication networks was not part of a public discussions. The reason is that until recently these systems were not so heavily involved into driver security. Currently start of these discussions seems unavoidable. In this article authors presented basic means of attacking CAN communication network within the vehicle and possible consequences. Some possible means of protection before these attacks were described. This issue was analyzed mainly in terms of possible legislation activities to enforce security procedures for civilian, governmental and military vehicles.

Keywords: *Automotive CAN network, safety, protection, microprocessor-based systems*

Bibliografia

Opracowania

[Bosch GmbH] *CAN – das Netzwerk für die Elektronik im Kraftfahrzeug*, [materiały reklamowe], Stuttgart 1999.

[Lawrenz] Lawrenz Wolfhard, *CAN System Engineering: From Theory to Practical Applications*, New York 2013.

Internet

[Illera, Vidal] Illera Alberto Garcia, Vidal Javier Vasquez, *What happened in my car*, https://www.blackhat.com/docs/asia-14/materials/Garcia-Illera/Asia-14-Garcia-Illera-Dude-WTF-In-My-Can.pdf.

[ISO 11898-1:2003] ISO 11898-1:2003, *Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signaling*, www.iso.org.

[ISO 11898-2:2003] ISO 11898-2:2003 *Road vehicles – Controller area network (CAN) – Part 2: High-speed medium access unit*, www.iso.org.

[ISO 11898-3:2006] ISO 11898-3:2006 *Road vehicles – Controller area network (CAN) – Part 3: Low-speed, fault-tolerant, medium-dependent interface*, www.iso.org.