Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 007.5
DOI: https://doi.org/10.24867/29IH02Vujic

SAJBER BEZBEDNOST U AUTOMOBILSKOJ IDUSTRIJI

CYBERSECURITY IN AUTOMOTIVE

Zoran Vujić, Vladimir Rajs, *Fakultet tehničkih nauka, Novi Sad*

Oblast – MEHATRONIKA

Kratak sadržaj – *U ovom radu prestavljen je opis algoritama koji se koriste u sajber bezbednosti. Opisane su funkcionalnosti i osobine koje treba da ima proizvod razvijen za automobilsku industriju kao i razlog njihove implementacije.*

Ključne reči: *Arhitektura, HSM, SHE, ključ, enkripcija, dekripcija, potpisivanje, heš, Autosar, secure boot, dijagnostika*

Abstract *–This paper presents a description of algorithms used in cybersecurity. The functionalities and characteristics that a product developed for the automotive industry should have, as well as the reasons for their implementation are described.*

Keywords: *Architecture, HSM, SHE, key, encryption, decryption, signing, hash, Autosar, secure boot, secure diagnostics*

1. UVOD

Sve veće oslanjanje vozila na povezanost na mreži kao i sve veći broj povezanih elektronskih uređaja i senzora u vozilu, u automobilskoj industriji, unosi dodatni rizik od neovlašćenog pristupa i zloupotrebe vozila.

Ovaj trend je doveo do sve većeg broja nesreća koje su izazvane neovlašćenim pristupom vozilu preko računara.

Iz ovog razloga napisan je standard, *ISO/SAE 21434*, koji se odnosi na sajber bezbednost u automobilskoj industriji i nadovezuje se na standard o sigurnosti, *ISO 26262*. Takođe, uvedena je regulacija, *UN R155*, kojom se obezbeđuje prisustvo sistema upravljanja sajber bezbednosti. U suštini, ova regulacija obezbeđuje da je projekat razvijan u skladu sa svim normama vezanim za sajber bezbednost.

2. Svojstva sajber bezbenodsti

Tri najbitnija svojstva sajber bezbednosti su poverljivost, autentičnost i integritet.
Poverljivost znači da čuvamo informaciu, poruku ili podatke u tajnosti. Drugim rečina, samo oni za koje je namenjena poruka mogu da je čitaju. Za sve ostale ona je nečitljiva.
Autentičnost govori da li su podaci poslati od onog entiteta od koga su i trebali da budu poslati.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Vladimir Rajs, van. prof.

Integritet govori da li su podaci ili poruka promenjeni od strane nekog trećeg lica. Obezbeđivanjem integriteta nad podacima omogućava se da se zna ukoliko je neko manipulisao podacima i menjao ih.

3.Bezbednosni algoritmi

3.1 Ključ

Ključevi u kriptografiji su nizovi karaktera generisani nasumično ili matematičkim algoritmima. Oni omogućavaju siguran prenos podataka, autentifikaciju, čuvanje poverljivih informacija i njihov integritet.
Jačina enkripcije zavisi od sigurnosti ključa, što uključuje algoritam generacije, veličinu ključa, način generacije i proces razmene ključeva. Ključevi se koriste za enkripciju podataka i potpisivanje digitalnih sertifikata.
Postoje asimetrični i simetrični ključevi. Bezbedna generacija i upravljanje ključevima uključuje izbor snažnih algoritama i sigurno skladištenje. Infrastruktura javnih ključeva (*engl. Public Key Infrastructure – PKI*) je često korišćena za ove svrhe.
Duži ključevi pružaju veću sigurnost, ali su sporiji za procesiranje.

3.2 Enkripcija

Enkripcija je ključna za bezbednu komunikaciju između dva uređaja putem nesigurnog kanala komunikacije. Ako se poruka pošalje nešifrovano, može biti presretnuta ili izmenjena, što može dovesti do ozbiljnih posledica, kao što su neovlašćeno kočenje ili ubrzavanje vozila. Enkripcijom se poruka pretvara u nečitljiv niz karaktera pomoću ključa. Samo uz pravi ključ poruka može biti dešifrovana.

Slika 1. Primer simetrične enkripcije

Simetrična enkripcija koristi isti ključ za enkripciju i dekripciju, što zahteva razmenu ključa između pošiljaoca i primaoca. Problem nastaje ako ključ bude presretnut.
Apsimetrična enkripcija koristi par ključeva: javni za enkripciju i privatni za dekripciju. Primalac generiše oba ključa, zadržava privatni i deli javni. Poruke enkriptovane javnim ključem može dekriptovati samo privatni ključ, čime se obezbeđuje sigurnost komunikacije.
Razlike između simetrične i asimetrične enkripcije:

Simetrična enkripcija:

- Koristi se jedan ključ za enkripciju i dekripciju
- Zahteva manje procesorskog vremena
- Manje bezbedna

Asimetrična enkripcija:

- Koristi dva ključa za enkripciju i dekripciju
- Zahteva dosta više procesorskog vremena
- Bezbednija od simetrične enrkipcije

Kombinacija simetrične i asimetrične enkripcije koristi se za efikasniju komunikaciju. Pošiljalac enkriptuje novi simetrični ključ javnim ključem primaoca, koji zatim koristi taj ključ za enkripciju i dekripciju poruka.

3.3 Kriptografski algoritam- HEŠ

Hešovanje je kriptografski algoritam koji pretvara ulazni tekst u jedinstveni, deterministički niz karaktera fiksne dužine. To je jednosmerni proces, što znači da se ne može dobiti originalni tekst iz heš vrednosti.

CRC32 je poznati heš algoritam za proveru integriteta podataka, ali nije pogodan za sajber bezbednost zbog svoje male dužine (4 bajta) i mogućnosti pronalaženja različitih ulaznih vrednosti koje daju isti izlaz.

SHA-256 je najčešće korišćen heš algoritam u sajber bezbednosti. Njegov izlaz je uvek 256 bita (32 bajta). Ovaj algoritam obezbeđuje da bilo koja promena ulaznih podataka daje potpuno drugačiji heš, i praktično je nemoguće naći različite ulazne vrednosti koje daju isti izlaz.

Hešovanje se koristi u bazama podataka za čuvanje lozinki. Lozinke se čuvaju kao heš vrednosti, i prilikom prijave korisnika, uneta lozinka se hešuje i upoređuje sa sačuvanom heš vrednošću. Na taj način, čak i ako neko neovlašćeno pristupi bazi, heš vrednosti lozinki su beskorisne, jer se ne može dobiti originalna lozinka iz heš vrednosti.

3.4 Digitalni potpis

Digitalni potpis je metoda za potvrdu identiteta pošiljaoca. U komunikaciji, pošiljalac generiše par ključeva – privatni i javni. Poruka se potpisuje privatnim ključem koristeći algoritam potpisivanja, a zatim se šalje primaocu zajedno sa potpisom. Primalac koristi javni ključ pošiljaoca za verifikaciju potpisa.
Potpisivanje se radi na heširanoj vrednosti poruke, ne na celoj poruci, zbog uštede vremena. Primalac hešuje poruku i dekriptuje potpis javnim ključem pošiljaoca, upoređujući dva heša. Ako se poklapaju, poruka je autentična i nije izmenjena.
Digitalni potpis osigurava autentifikaciju pošiljaoca i integritet poruke. Ako se poruka izmeni, verifikacija potpisa neće biti uspešna. Takođe, digitalni potpis pruža dokaz o identitetu pošiljaoca, autentičnosti i integritetu poruke, što onemogućava pošiljaoca da negira slanje poruke (ne-odricanje).

3.5 Kod za autentifikaciju poruke

Kod za autentifikaciju poruke (*engl. Message Authentication Code – MAC*) se koristi za autentifikaciju porekla i integriteta poruke. *MAC* koristi tajni simetrični ključ i podatke poruke kako bi generisao fiksni kod koji se dodaje na kraj poruke.
Kada primalac primi poruku, on izračunava *MAC* koristeći isti algoritam i ključ. Ako se izračunati *MAC* poklapa sa primljenim, poruka je autentična i nije izmenjena.
MAC algoritam zahteva tajni ključ poznat samo pošiljaocu i primaocu. Bez tog ključa, nije moguće kreirati ispravan *MAC*. Najčešće korišćeni *MAC* algoritmi su *CMAC* i *HMAC*.

4.INFRASTRUKTURA JAVNIH KLJUČEVA

4.1 Definicija infrastrukture javnih ključeva

Infrastruktura javnih ključeva (*PKI*) je sistem alata koji omogućava bezbednu razmenu podataka preko interneta putem kreiranja i upravljanja javnim ključevima za enkripciju. *PKI* je ugrađen u sve *web* pretraživače i osigurava sigurnost javnog internet saobraćaja. Organizacije ga koriste kako bi osigurale sigurnu komunikaciju unutar i izvan svojih okvira. Ključevi su osnovna komponenta *PKI* sistema, koriste se za šifrovanje podataka i autentifikaciju. *PKI* funkcioniše kroz upotrebu sertifikata i ključeva. Javni ključ se koristi za enkripciju poruka, dok se privatni ključ koristi za dešifrovanje istih. Sertifikati izdati od strane autoriteta za sertifikaciju (*engl. Certificate Authority – CA)* omogućavaju osobi ili uređaju da zna da komunicira s nekim ko je ovlašćen.

4.2 Digitalni sertifikat

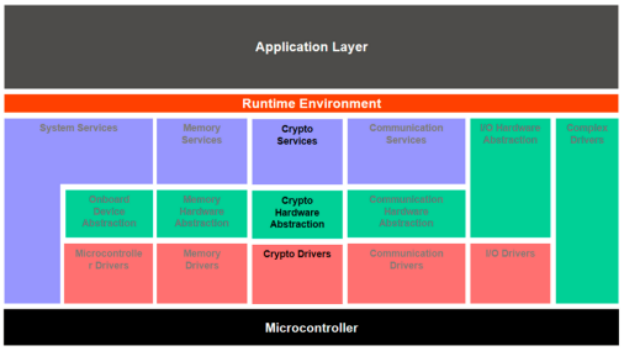
Digitalni sertifikat je digitalni dokument ili elektronski identitet koji potvrđuje autentičnost uređaja, servera ili korisnika koristeći kriptografiju i infrastrukturu javnih ključeva. Korišćenje digitalnih sertifikata za autentifikaciju omogućava organizacijama da osiguraju da se na njihove mreže mogu povezati samo provereni uređaji i korisnici. Još jedna česta upotreba digitalnih sertifikata je potvrda autentičnosti internet stranica pretraživaču, poznata kao SSL sertifikat. Sadržaj digitalnog sertifikata obuhvata identifikacione informacije kao što su korisničko ime, kompanija, IP adresa uređaja ili serijski broj, kao i kopiju javnog ključa kreatora sertifikata. Javni ključ se izdaje od strane autoriteta za sertifikaciju (*CA*), koji potpisuje sertifikat kako bi se potvrdio identitet uređaja ili korisnika u svrhu autentifikacije. Primjer digitalnog sertifikata je *X.509* sertifikat koji se često koristi u automobilskoj industriji.

4.3 Autoritet za sertifikaciju

Autoritet za sertifikaciju (*engl Certificate Authority – CA*) je entitet koji čuva, potpisuje i izdaje digitalne sertifikate za autentifikaciju korisnika, servera ili uređaja. Ovi sertifikati potvrđuju vlasništvo javnog ključa i omogućavaju drugim stranama da provere validnost potpisa i autentičnost. CA se posmatra kao treća strana koja je pouzdana i kojoj veruje nosilac sertifikata i strane koje se oslanjaju na sertifikate za autentifikaciju. On takođe može obezbediti generisanje para ključeva u slučaju da organizacija ili korisnik nemaju tu mogućnost. Sertifikati koje izdaje *CA* slede standarde *X.509* ili *EMV* i predstavljaju važan deo infrastrukture javnih ključeva (*PKI*).

5. AUTOSAR *CRYPTO STACK*

AUTOSAR (AUTomotive Open System Architecture) je partnersko udruženje na globalnom nivou koje se bavi razvojem u automobilskoj industriji. Glavni cilj AUTOSAR partnerskog udruženja je pružanje vodećih rešenja za softverske platforme kroz standardizaciju osnovnih sistemskih funkcija i interfejsa. Ovaj okvir omogućava efikasan razvoj embedded softvera i aplikacija koje podržavaju zadatke vezane za osnovne funkcionalnosti u automobilima tokom razvoja vozila.

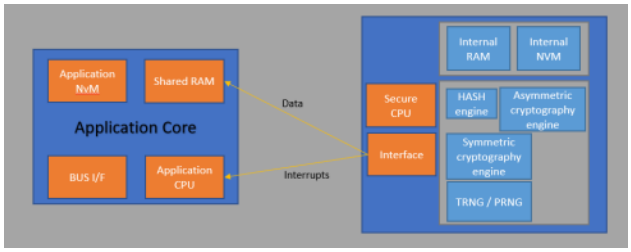


Slika 2. AUTOSAR crypto stack arhitektura

Na najnižem nivou, *MCAL (engl. Microcontroller Abstraction Layer)*, nalazi se Kripto Drajver. Ovi moduli sadrže konkretne softverske ili hardverske implementacije kriptografskih servisa.
Kripto interfejs modul se nalazi na nivou Hardverske Apstrakcije (*Hardware Abstraction Layer*). On nam obezbeđuje generičke interfejse.
Kripto servis menadžer nalazi se u servisnom nivou (*Service Layer*). On nudi aplikativnim komponentama standardizovan pristup kriptografskim servisima preko *RTE*.

6. HARDVERSKI BEZBEDNOSNI MODUL

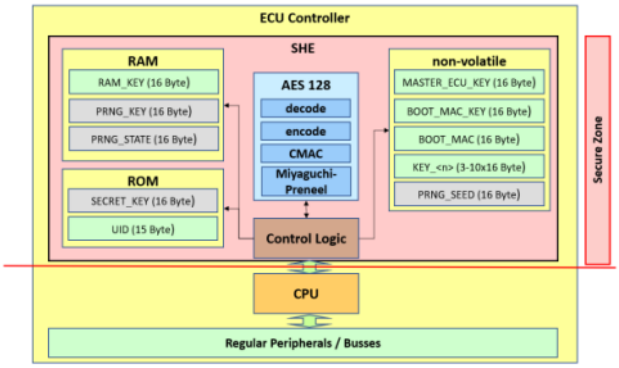
Hardverski bezbednosni modul (*engl. Hardware Security Module – HSM*), je poseban hardverski periferal na sistemu na čipu (*engl. System on Chip – SoC*) koji je zadužen za izvršavanje bezbednosnih servisa. On u suštini predstavlja bezbednosno jezgro (core) na *SoC*



Slika 4. Arhitektura *HSM*

6.1 Bezbednosno hardversko proširenje

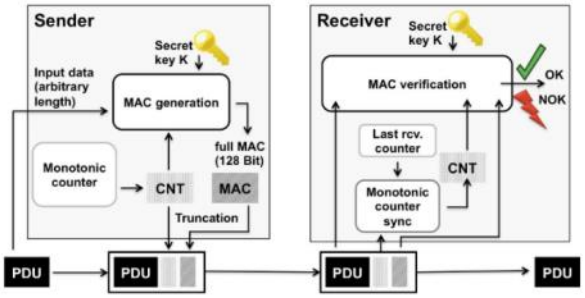
Bezbednosno hardversko proširenje (*engl. Secure Hardware Extension – SHE*) je proširenje na čipu bilo kog mikrokontrolera. Njegova svrha je prenos kontrole nad kriptografskim ključevima iz softverskog u hardverski domen, čime se ključevi štite od softverskih napada. Jednostavnije je i jeftinije od *HSM*.



Slika 5. Logička struktura *SHE*

7. SecOC

SecOC (Secure Onboard Communication) je AUTOSAR bezbednosna arhitektura koja za cilj ima da zaštiti komunikacije između različitih ECU u vozilu od sajber napada.
Ovaj modul obezbeđuje funkcionalnost neophodnu za autentifikaciju, proveru integriteta i *freshness value* komunikacije bazirane na *PDU* između dva *ECU* na mreži.



Slika 6. Provera poruke *SecOC* modula

Freshness value služi za sprečavanje ponovnog napada (*replay attack*). Ako napadač snimi poruku na mreži, mogao bi je ponovo slati i autentifikacija bi prošla, što bi omogućilo manipulaciju uređajima na mreži. Freshness value je deo bezbednog *PDU* i može biti implementiran na dva načina:

- Brojački mehanizam: Brojač se inkrementira za svaku poruku, a primalac očekuje vrednost brojača za 1 veću od prethodne.
- Vremenski mehanizam: Vrednost se zasniva na vremenu slanja poruke plus interval. Vremena pošiljaoca i primaoca moraju biti sinhronizovana.

Freshness value se koristi u kalkulaciji *MAC*, što sprečava ponovni napad istom porukom jer će se promenom *freshness value* promeniti i *MAC*. Za isti *PDU*, bezbednosni *PDU* će uvek biti različit zbog različitih *freshness value* i *MAC*. Svaki *PDU* ima svoj *freshness value* koji se menja pri slanju i prijemu poruke. Kod brojača, pošiljalac inicijalizuje freshness value na 1, a primalac na 0.

8. *SECURE BOOT*

Bezbedno pokretanje (*engl. Secure boot*) mehanizam mora biti utisnut u boot lanac da autentifikuje i potvrdi firmware pre nego što dozvoli njegovo izvršavanje od veoma rane faze. Na ovaj način se obezbeđuje

autentičnost, a integritet firmwarea se održava i u kasnijim fazama softvera. Napadač može pokušati da izmeni ili reprogramira sadržaj firmwarea tako što će u potpunosti promeniti njegov kod ili ubaciti deo svog koda koji može biti izvršen umesto autentifikovanog. Napadi se mogu desiti korišćenjem informacija zasnovanih na fizičkoj implementaciji sistema kao što su napadi sa sporednih kanala (*Side-channel attacks*) uključujući i aktivne napade poput ubrizgavanja grešaka (*Fault injections*). Izvođenje takvih napada tokom rane faze pokretanja može dovesti do potpunog ugrožavanja bezbednosti sistema.

9. PODACI O VALIDNOSTI INTEGRITETA

Podaci o validnosti integriteta (*engl. Integrity Validation Data – IVD*) služe da bi se potvrdila validnost trenutnog softvera koji se izvršava, kao i dijagnostičkih parametara. Najčešći metod za proveru integriteta je hešovanje kompletnog softvera na strani uređaja i upoređivanje dobijene heš vrednosti sa očekivanom. Korišćenjem sigurnih heš algoritama (kao što su SHA i MD5) za dobijanje *IVD* vrednosti, obezbeđujemo da ukoliko se poklapaju dobijena i očekivana heš vrednost, možemo sa sigurnošću reći da su podaci nad kojima je rađen algoritam isti, odnosno da su softver i parametri oni koje očekujemo. Na ovaj način, ukoliko se promeni makar i jedan bit softvera koji se izvršava, dobijena heš vrednost će biti potpuno drugačija u odnosu na očekivanu.

10. SIGURNA DIJAGNOSTIKA

Prema *UDS* (*engl. Unified Diagnostic Standard – UDS*) standardu *ISO 14229*, svi programabilni serveri koji imaju podatke vezane za emisiju štetnih gasova, sigurnost ili neke druge podatke koji se mogu ukrasti i zloupotrebiti moraju da implementiraju bezbednosne servise za dobijanje tih podataka preko dijagnostike koristeći seme i ključ (*engl. Seed and Key*) odnosno bezbednosni pristup (*engl. Security Access*). Bezbednosnim pristupom se mora osigurati i programiranje/flashovanje uređaja i ono mora biti aktivno odmah po napuštanju uređaja iz proizvodnje. Svrha servisa sigurne dijagnostike je pružanje sredstava za pristup podacima i/ili dijagnostičkim uslugama koje imaju ograničen pristup iz sigurnosnih, emisionih ili bezbednosnih razloga. Dijagnostičke usluge za preuzimanje/dodavanje rutina ili podataka u server i čitanje određenih lokacija u memoriji sa servera su situacije gde može biti potreban bezbednosni pristup. Neispravne rutine ili podaci preuzeti u server mogli bi potencijalno oštetiti elektroniku ili druge komponente vozila ili ugroziti usklađenost vozila sa standardima emisije, bezbednosti ili sigurnosti. Dva najbitnija servisa za pristup bezbednim sesijama su servisi 27_{16} i 29_{16} ($_{16}$ označava da je broj servisa izražen u heksadecimalnom obliku).

11. ZAKLJUČAK

Prikazane su osobine i karakteristike sajber bezbednosti koje treba da poseduje proizvod namenjen za automobilsku industriju. Spoj poznavanja algoritama i specijalno dizajniranog hardvera nam omogućava da realizujemo sve bezbednosne koncepte da bi se rizik od napada smanjio na minimum. Bliže su opisani algoritmi i razlog njihovog korišćenja. Opisana je upotreba algoritama u svrsi implementacije različitih funkcionalnosti i prikazano kako to može da izgleda u praksi pri realizaciji realnog projekta. Projekat se razvija u skladu sa predefinisanim standardima i specifikacijama da bi se dostigao željeni nivo bezbednosti i rizik i odgovornost smanjili na minimum.

12. LITERATURA

[1] https://en.wikipedia.org/wiki/Message_authentication_code

[2] https://learn.microsoft.com/en-us/windows/win32/seccertenroll/about-x-509-public-key-certificates

[3] https://www.autosar.org/fileadmin/standards/R22-11/FO/AUTOSAR_TR_SecureHardwareExtensions.pdf

[4] https://www.autosar.org/fileadmin/standards/R19-11/CP/AUTOSAR_SWS_SecureOnboardCommunication.pdf

[5] https://www.autosar.org/fileadmin/standards/R22-11/CP/AUTOSAR_EXP_UtilizationOfCryptoServices.pdf

[6] https://www.vector.com/int/en/products/solutions/safety-security/automotive-cybersecurity/security-manager/#c233594

[7] Road vehicles – Unified diagnostic Services (UDS), UDS_ISO_14229-1-01_02_2020

Kratka biografija:

Zoran Vujić rođen u Novom Sadu 1997. god. Diplomski rad na Fakultetu tehničkih nauka iz oblasti mehatronike odbranio je 2020. godine.

Vladimir Rajs rođen je 1982. godine u Apatinu. Diplomirao je 2007, a doktorirao 2015. godine na Fakultetu tehničkih nauka u Novom Sadu. Od 2016. godine je bio zaposlen kao docent, od 2021. kao vandredni profesor na Departmanu za elektroniku, energetiku i telekomunikacije FTN-a.