Naslov seminarskog rada

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Prvi autor, drugi autor (treći autor)
kontakt email prvog, drugog (trećeg) autora

9. april 2015.

Sadržaj

1 Uvod

2 Izazovi

[1]

Svaki računarski sistem može biti preplavljen propustima i slabostima koje napadač može da iskoristi ako je povezan na sistem. Elektronskim kontrolnim jedinicama (EKJ ili ECU na engleskom) nije lako pristupiti van vozila, te implementacija bezbednosnih mehanizama u računarskim mrežama u automobilima nije bila velika briga proizvođača.

Umrežavanje je trend današnjice. Moderna vozila često poseduju interfejse koji omogućavaju ili žičanu ili bežičnu komunikaciju. Ovime su mreže u automobilima prestale da budu zatvorene i sajber-napadi su postali realnost.

2.1 Razlozi za napade

Razmotrimo prvo koje sve motive napadači računarskih mreža u automobilima mogu imati.

Krađa

Napadač može da iskoristi neki prisutni propust u bežičnoj komunikaciji i na taj način tiho i neprimetno otključa automobil i zatim deaktivira alaram.

Elektronska podešavanja

Napadač je upravo vlasnik ciljanog automobila. Vlasnik može da pristupi kodu ili podacima i promeni ih. Na primer, može da smanji kilometražu automobila pre prodaje, izvrši podešavanje motora i dobije više snage ili instalira nedozvoljene programe u komandnoj tabli. Takođe, mogu se instalirati jeftine AFTERMARKET komponente umesto skupljih koje je odobrio proizvođač.

Sabotaža

Sabotaža podrazumeva deaktivaciju EKJ, menjanje njihovog softvera ili dos (denial of service) napade na mrežu. Posledice ovih napada se protežu od minornih (zaključavanje klima uređaja) do potencijalno smrtonosnih (zaključavanje kočnica). Ali čak i napadi koji uzrokuju samo male neprijatnosti mogu znatno da utiču na reputaciju proizvođača.

Intelektualna krađa

Napadač može da pokuša da pristupi poverljivim informacijama o EMBEDDED mreži ciljanog vozila. To se može postići prisluškivanjem magistrale ili pristupanjem izvornom kodu neke EKJ. Ovakvi napadi mogu da omoguće proizvodnju falsifikovanih EKJ, kao i širenje informacija o propustima u bezbednosti drugim napadačima.

Povreda privatnosti

Sa povećanjem broja elektronskih komponenti, povećava se i količina privatnih informacija koje te komponente skupljaju. Napadač može da pristupi telefonskom imeniku vlasnika kao i istoriji poziva, istoriji GPS koordinata ili omiljenim radio frekvencijama.

Intelektualni izazovi

Mnogi napadači su prosto motivisani izazovom preuzimanja kontrole nad vozilom. Postoje mnogi primeri ovakvih napada kroz istoriju računarstva.

Naravno, jedan napadač može imati i više motiva.

2.2 Unutrašnji napadi

Kao što je ranije pomenuto, neki bezbednosni mehanizmi su implementirani u posotjeće računarske mreže u vozilima. Bezbednost je postala značajan problem s obzirom da posledice napada mogu biti veoma ozbiljne, a napadi se mogu lakše izvesti zahvaljujući rapidnoj evoluciji mreža.

Ranjivost magistrale

Već su prikazane ranjivosti koje postoje u trenutnim protokolima, sa fokusom na CAN. Iako neke EKJ imaju specifične bezbednosne mehanizme (kao što je autentikacija uređaja), pokazano je da CAN ne može da garantuje sledeće osobine:

- Poverljivost:
  Dizajn je takav da se svaka poruka poslata na CAN i fizički i logički šalje (BROADCAST) svakom čvoru. Ovo omogućava zlonamernim čvorovima da prisluškuju magistralu i čitaju sadržaj svakakog okvira (FRAME).
- Autentikacija:
  CAN okvir ne podrazumeva polje za autentikaciju svog pošiljaoca. Dakle, svaki čvor može da pošalje poruku koju bi trebalo da može da šalje samo jedan specifičan čvor.
- Dostupnost:
  Veoma je lako izazvati dos napad na magistrali. Na primer, neka jedinica može da preplavi magistralu okvirima visokog prioriteta i time zaustavi transmisije ostalih EKJ.
- Integritet:
  CAN koristi CRC (cyclic redundancy check) da proveri da li je poruka promenjena usled greške, ali ovaj mehanizam ne može da spreči napadača koji želi da promeni ispravnu poruku jer je lako napraviti ispravan CRC za lažnu poruku.

Lokalni napadi

Napadi na magistralu se mogu izvršiti ili povezivanjem uređaja na magistralu ili preko OBD (eng. On Board Diagnostics) porta. OBD predstavlja sposobnost vozila da identifikuje i prijavi postojeće probleme. Preko ovog porta se može prisluškivati komunikacija na magistrali ali mogu se slati i okviri.

Postoje mnogi dokumentovani primeri napada bazirani na direktnom pristupu unutrašnjoj mreži. Napad počinje iz 'black-box' perspektive (NJEGOV 9 OVDE). Na taj način, napadač se upoznaje sa značenjem okvira i njihovih identifikatora. Zatim, zlonamerna EKJ može da ponovi kontrolne instrukcije i pošalje ih drugim EKJ, predstavljajući se kao validan

izvor instrukcija (NJEGOV 10 oVDE). Neke EKJ je čak moguće i reprogramirati kroz mrežu (NJEGOV 11 OVDE), čime se vozilo ostavlja u kompromitovanom stanju.

Nilson i Larson uvode ideju virusa koji napada mreže u vozilima, koji se aktivira tek kad su određeni uslovi postignuti (npr. poslat je određeni okvir) (NJEGOV 12 OVDE).

Koscher (PREVOD) u svom radu (NJEGOV 11 OVDE) prikazuje način na koji se može napasti EKJ koja se nalazi na delu magistrale koji se razlikuje od ulazne tačke napadače. Napad se može izvršiti tako što se prvo ciljaju i reprogramiraju EKJ koje predstavljaju kapiju između magistrala, tako da one EKJ koje se nalaze na delu magistrale male brzine mogu da šalju poruke EKJ na brzim delovima magistrale, čija je bezbednost kritična.

Dakle, ako napadač kontroliše makar jedan čvor mreže, trenutna arhitektura i protokoli omogućavaju da preuzme kontrolu nad bilo kojom EKJ vozila. Mogao bi se postaviti argument da je potreban direktan, fizički pristup kako bi se izvršio bilo koji od navedenih napada. Dakle, napadač bi prvo morao da ima pristup vozilu a zatim da ugradi uređaj u magistralu. U većini slučajeva, brže i lakše bi bilo napasti vozilo ne-elektronski (npr. lakše je iseći kočnice nego hakovati odgovarajući EKJ).

Sa druge strane, moderni automobili poseduju mogućnost bežične komunikacije. Napadačima više nije potreban direktan pristup ciljanom vozilu. U sledećem odeljku će biti prikazani takvi napadi.

2.3 Spoljašnji napadi

2011. godine, Checkoway je uspeo da REMOTELY reprodukuje napade opisane u (NJEGOV 11 OVDE) pronašavši i iskoristivši ranjivosti u interfejsu za komunikaciju (NJEGOV FIGURE 1), bez fizičkog pristupa samoj mreži.

Spoljašnji napadi mogu biti grupisani na sledeći način, po distanci: indirektan pristup, bežični pristup malog dometa i bežični pristup širokog dometa. Svaki od ovih pristupa će u nastavku biti opisan i biće dati neki mogući scenariji napada.

Indirektan pristup

U ovom odeljku, pažnja je posvećena napadima koji se oslanjaju na kompromitovanim THIRD-PARTY uređajima koji će biti povezani sa vozilom. Za razliku od unutrašnjih napada, povezivanje sa mrežom ne čini napadač, već vlasnik vozila.

- OBD port:

  Ranije je prikazano kako se sam OBD port može koristiti u napadima. U ovom slučaju, meta napada je uređaj za dijagnostiku koji je priključen na port. Moguće je kompromitovati PASS THRU uređaj, koji je priključen na port i kontroliše se putem laptopa preko WiFi-a: ranjivosti u API-u za komunikaciju su omogućile da se ubaci (INJECT) shell skripta u taj uređaj preko drugog laptopa na istoj WiFi mreži. Zatim bi uređaj emitovao zlonamerne pakete preko mreže vozila svaki put kab bi bio priključen (NJEGOV 3 OVDE).

- CD player:
  U radu (NJEGOV 3 OVDE) su identifikovane dve ranjivosti u CD PLAYERu. Ubacivanje CD-a na kome se nalazi datoteka specifičnog imena može da zavara PLAYER da pomisli da je u pitanju neko fabričko ažuriranje. Uređaj će zatim instalirati novi, maliciozni softver. Još jedan propust je u dekodovanju WMA datoteka - moguće je napraviti audio datoteku koja će izazvati slanje poruka preko magistrale dok je PLAYER čita. Drugi primer napada je mnogo ozbiljnija pretnja, s obzirom da su audio datoteke, deljene preko peer-to-peer mreža, često zaražene zlonamernim softverom.
- USB port:

Napadi malog dometa

- Bežično povezivanje sa mobilnim uređajem:
- Komunikacija između vozila:
- TPMS:
- Bežično otključavanje:

Napadi širokog dometa

- Telefonija:
- Web browsing:
- App store:

USB port: Several scenarios can be devised. First, cases similar to the previous one are plausible, where the car media player accesses a corrupted file stored on a USB key. Another possibility would be through the connection of a compromised device (like a smartphone or a mp3 player) which would then perform an attack against the ECU it is connected to. If such an attack has not been reported yet, previous examples of attacks against a mobile phone (for example via bluetooth1 or after the installation of an installation containing a trojan horse) make this a viable scenario. 2) Short range attacks: This category regroups attacks that use short-range wireless communication technologies. The attacks can be direct, if the attacker tries to directly target a car's communication module or indirect if he targets a driver's device that is already able to connect to the car (e.g., a smartphone). Wireless pairing of mobile devices: Modern vehicles can sometimes be paired with compatible mobile devices. For example, the driver can connect his phone via Bluetooth and use his car's sound system as a hands free kit. However, the implementation of such wireless protocols into the car can be faulty. Exploiting such vulnerabilities can lead to the retrieval of data stored into the communications unit, the ability to eavesdrop on the conversations (be they phonecalls or conversations between the passengers) or even the compromission of the ECU [3] (and therefore the network). Car-to-car communications: Communications between a vehicle and other vehicles or roadside infrastructures are probably the next big evolution in the domain of road transport. Indeed, in a few years probably, a car will be able to communicate its status to the neighbouring vehicles. This would for example allow a car to alert its driver in case of an imminent danger (emergency braking

of a car ahead, incoming vehicles at a crossroad, etc.) or even to automatically adapt to the new conditions. A detailed risk analysis for intervehicular communications can be found in [13]. Among these risks, we can cite the eavesdropping on the communications, the emission of fake data to a vehicle in order to trigger an unappropriate reaction, and of course a potential compromission of the ECU responsible for car-to-car communications. TPMS: Tire Pressure Monitoring System is composed of a pressure sensor inside the tire that sends its data to a dedicated ECU located on the CAN via a radio frequency emitter. TPMS are now mandatory in the US, in Europe and soon in Japan. In [14], attacks against a TPMS allowed the team to eavesdrop on it from up to 40 meters and send spoofed messages to the monitoring ECU, causing it to turn on tire pressure warning lights at inappropriate times. Wireless unlocking: Many cars now implement a remote unlocking of their doors or alarms. While some encryption is applied to such instructions sent over the air, it can be cracked, or bypassed. For example, documented attacks against KeeLoq, a block cipher used by several manufacturers, can be found in [15] or [16]. Moreover, Passive Keyless Entry and Start (PKES) systems allow the drivers to unlock and start their cars while keeping their keys in their pockets. In [17], a team was able to perform relay attacks on PKES systems of ten different car models. As a result, by placing an antenna close to the key holder (within a 8m radius) and another near the targeted car, they were able to unlock it then start its engine while the keys were actually 50 meters from the car. As evidenced by our last example, the šhort"range of the aforementioned wireless protocols can sometimes be extended through the use of relays or more powerful antennas. For example, an attack carried via bluetooth has reportedly been made from a distance of over one mile2 . 3) Long-range direct attacks: This category regroups attacks carried over long-range wireless communica- tion technologies. Telephony: Following the discovery of several vulnerabilities in the telematic unit, Checkoway et al. [3] successfully made it execute custom code downloaded through the 3G network, effectively compromising the vehicle. Web browsing: In the event that a vehicle embeds a web browser, possible exploits similar to those found on traditional computers and mobile devices are to be considered (e.g., buffer overflow, code injection, etc.). 4) Long range indirect attacks: Finally, we describe here attacks that require a long-range transmission channel and also the compromission of an intermediary device. 2http://trifinite.org/trifinite_stuff_lds.html App store: In a trend similar to what can be found on the smartphones, some car manufacturers already provide, via the firm online store (similar to the Apple Appstore or the Google Play Store), a selection of downloadable applications for the multimedia unit of their cars. A successful attack against the online store, or a program sold on such a store actually containing a trojan horse (such programs have already been found on the Appstore and the Play Store3) would have serious large scale consequences. Side channel triggers: In [3], an hypothetical scenario is devised in which a backdoor is installed into an ECU of a vehicle compromised through any of the previously described attacks. From that moment on, broadcasts of certain signals (for example via RDS4) will trigger the execution of a series of instructions in any compromised vehicle in range of these broadcasts. Catastrophic scenarios can be imagined by combining such techniques with a great amount of previously infected vehicles. App store: In a trend similar to what can be found on the smartphones, some car manufacturers already provide, via the firm online store (similar to the Apple Appstore or the Google Play Store),

a selection of downloadable applications for the multimedia unit of their cars. A successful attack against the online store, or a program sold on such a store actually containing a trojan horse (such programs have already been found on the Appstore and the Play Store3) would have serious large scale consequences.

2.4 Mehanizmi zaštite

As previously seen, cars are now able to communicate via numerous channels, which can become potential entry points into the embedded network for an attacker. If documented examples of more and more advanced attacks appeared during the last few years, countermeasures are also being developed. In this section, we first present the constraints that must be taken into account while designing security solutions for the automotive environment. Then, we describe the techniques currently being developped to enforce security properties in the automotive networks. We begin with the wireless communications protocols and then focus more specifically on internal defense mechanisms. While this survey makes no claim of comprehensiveness (and can be completed by similar works such as [18] or [5]) we however tried to the best of our knowledge to illustrate the different areas of research currently being explored. A. Constraints Even if usual computing security concepts and methods can be adapted to protect a connected car, important differences still remain and impact the design and set up of automotive security mechanisms. Wolf et al. [5] express the following constraints: Hardware: Most of a car's embedded computers have strong hardware limitations compared to current traditional computers or smartphones. With such limited computing power and memory, these ECUs are not able to perform advanced cryptographic functions allowing for strong encryption. However, the attacker's hardware may not have such limitations, so a too simple ciphering algorithm could easily be cracked and would therefore prove ineffective (and even counterproductive). Real time: Similarly, due to the limited computational power of an ECU, longer durations are required to run complex instructions. On the other side, automotive software must deal with real-time constraints, in particular the embedded applications must run in a given time to ensure the safety of the vehicle and its passengers. Therefore, any security mechanism must not impact signifi- cantly the embedded software performance. Autonomy: The driver's attention must overall be focused on the driving. Therefore, the protection mechanisms have to be as autonomous as possible and must only require the driver's attention in extreme situations. Physical constraints: Some ECUs must be able to sustain physical conditions (high temperatures, moisture, shocks. . . .) that would not be encountered by a traditional computing system. Lifecycle: The lifecycle of a vehicle (about twenty years) is longer than that of a computer. Embedded security systems must therefore be effi- cient throughout that duration. Therefore, to prevent obsolescence of security mechanisms, it is advisable to design them to allow an easy updating. Compatibility: Compatibility must be ensured in two aspects. First, in order to reduce the costs, a security architecture should be as compatible as possible with the currently used embedded technologies (retrocompatibility). Moreover, communications with external sources (devices or other vehicles) must not be hindered by the security mechanisms (interoperability). For example, two distinct car models should not be prevented from communicating because their protocols are incompatible. B. External communications protections As seen in the previous

section, one vulnerability into the management of the communications with an external device may be enough to entirely compromise the vehicle. Therefore, a first step in order to protect the embedded system would be to secure those channels. Among the attacks described in III-C, many were allowed by poor implementations of the targeted protocols, flaws in the programming of the involved applications (allowing for buffer overflows) or non-compliance with the manufacturer's specifications. Therefore, such attacks could have been theoretically prevented by strict compliance with good programming practices and by following the existing security recommendations about the communication protocols (for example, [19]). However, the complexity of today's embedded systems combined with the fact that ECUs come from different suppliers can make it almost impossible to check for the compliance with all relevant specifications. Therefore, the integration of additional defense mechanisms in order to secure the communications is essential. The manufacturers are now fully aware of such issues, as evidenced by the recent large-scale projects between industrial and academic partners. For example, European projects such as SEVECOM [20], PRESERVE [21] or EVITA [22] aim at designing secure communication architectures for internal or intervehicular communications. On a different topic, the goal of OVERSEE [23] is to devise a unified, open and secured multimedia interface managing all the communication protocols. C. Internal protections Regarding the security of the communications over the CAN bus, several solutions (not mutually exclusive) are being considered. We can classify them into three categories. • Cryptographic solutions to authenticate or encrypt the packets transmitted on a bus. • Solutions detecting anomalies occuring in the system. • Solutions to ensure integrity of the embedded software. 1) Cryptography: As seen in II, any message emitted on CAN is broadcast to all the nodes connected to the bus. Moreover, there is no proper way of authenticating the sender of a message. In order to overcome these issues, the implementation of cryptographic solutions on the CAN can enable ECU authentication, integrity checks and encryption of the emitted frames, preventing its reading by nodes not possessing the appropriate keys. Such features are for example proposed in the implementations described in [24], [25] or [26]. However, the computation required to perform strong enough encryption or decryption of the messages can be very time and resource consuming, which is an important issue in a real-time system such as a vehicle. This problem can be addressed by using a hardware module entirely dedicated to cryptographic operations in order to free the ECUs computational capacities. EVITA conceived such a device, called the Hardware Security Module (HSM), which exists in three models implementing various security features according to each ECU requirements [27]. [28] gives examples of a secure key exchange protocol and message encryption using the HSM and an ECU dedicated to key management. 2) Anomaly detection: Other works aim at monitoring the data transmitted between ECUs and assert their legitimacy. A simple and more safetyoriented example can be found in [29] where a module detects if the delay between two frames sent by the monitored ECU is too short, in which case the faulty ECU gets muted. Moreover, [30] proposed a system where, on every bus, each frame identifier is associated to only one ECU. In other words, such frames can only be sent by one particular ECU and therefore cannot legitimately be sent by the others. Then, whenever a message is emitted on the bus, each ECU checks if the frame identifier is one of its own. If it is the case and if the ECU itself is not the actual sender of the frame currently

being emitted, it immediately emits a high-priority alert frame to override the illicit emission. [31] uses a binary tainting tool to mark the data being used by the ECUs as they are processed and sent on the network. It is then possible to track the origin of malicious instructions in the system. However, this solution is currently quite resourceconsuming. Finally, some works are focusing on the deployment of intrusion detection (resp. prevention) systems (IDS, resp. IPS) in a similar fashion to those found in the traditional computing world. These systems can use two detection methods: • Signature-based: An alert is raised whenever a sequence of frames corresponds to a known signature stored in the system database. If a well defined signature base raises very few false positive, regular updates are required to enable the detection of newly discovered attack patterns. The eight sensors given and discussed in [32] monitoring different aspects of the frames being emitted on the CAN (see table III) can provide an example of the kind of rules required to monitor the bus. • Anomaly-based: This approach requires to define models representing all the possible normal behaviors of the monitored system. Then, anomalies are detected whenever the current state of the system deviates too much from the corresponding model. If such systems can theoretically detect previously unknown attacks, the high complexity of an automotive network makes it difficult to design a model precise enough to prevent false negatives while still allowing exceptional but perfectly legitimate situations. For example, [33] defines the notion of entropy on the CAN and tries to detect sudden deviations of said entropy compared to a reference set. If these examples of intrusion detection systems applied to an automotive context are still early proofs of concept, the idea seems promising. However, as reminded in IV-A, the automotive environment does not have the same constraints than a traditional computing network. For example, a car may not be able to update its software (and therefore an IDS signature base) as frequently as a computer. Similarly, as the embedded security systems need to be as autonomous as possible, automatic handling of a false positive could trigger an unnecessary intervention or even endanger the passengers safety. 3) ECU software integrity: Finally, means of ensuring that the vehicle's critical software cannot be affected by an attack are also considered. First, secure validation of an ECU code can be done in a way similar to the secure boot mechanisms [34] implemented in traditionnal computers. The definition of a trusted base in a vehicle can be done through security modules such as EVITA's HSM or a TPM (Trusted Platform Module) [35]. Ensuring integrity of the multimedia ECU is also one of the main goals of OVERSEE, which is accomplished through the use of a hypervisor (XtratuM5) in order to isolate critical software (allowed to write on the buses) from non trusted modules such as the external communication interfaces by putting them into distinct virtual machines. Therefore, should an attacker exploit a vulnerability in a wireless communication protocol, he will not be able to compromise the whole ECU and send messages on the bus (if the hypervisor is able to enforce a strict isolation policy).

V. CONCLUSION In this paper, we have seen that the lack of existing security mechanisms in the current automotive network architectures has become a serious issue with the addition of wireless communication capacities to the modern cars. Indeed, vulnerabilities in the modules handling such wireless protocols can allow an attacker to remotely access the vehicle embedded network and jeopardize the integrity of possibly every ECU on the network. Therefore, the design and implementation of automotive security mechanisms has become

a key issue for automotive manufacturers. We then presented several works aiming at enforcing security in automotive networks on three main aspects: • Encryption of the communications • Anomaly detection • Integrity of the embedded software Research on such topics is really intense today, as evidenced by the strong implication of manufacturers and academics into several large-scale projects whose results enable the current implementations of first security modules. However, there is still many work to do, especially as experiences from traditional computing remind us that such issues may never be completely solved.

Literatura

[1] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi. Survey on security threats and protection mechanisms in embedded automotive networks. In *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 1–12, June 2013.