Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 875

On the Fingerprinting of Electronic Control Units Using Physical Characteristics in Controller Area Networks

Marcel Kneib[1] and Christopher Huth[2]

Abstract: More and more connected features, like up-to-date maps or car-to-car communication, are added to our vehicles. Besides comfort and environmental benefits, those connections also enable attackers to cause high damages, as Miller and Valasek had shown with their remote hack of a Jeep Cherokee [MV15]. The exploited vulnerability caused a recall of 1.4 million vehicles. Such attacks are possible since no security mechanisms and no sender information are present in the Controller Area Network. Unfortunately, classical cryptographic algorithms cannot be added easily, due to its small payload size. A promising opportunity to increase security is to exploit physical information included in the received messages by extracting fingerprints. These allow to identify the sender of received messages, what can enhance detection or prevention of attacks. In the following, we impart the needed background and give an overview of the two known approaches to expand the Controller Area Network with sender identification.

Keywords: In-Vehicle Network; CAN; Intrusion Detection System; Fingerprinting ECU; Security

1 Motivation

The growing expansion of mobile networks leads to the integration of Internet-based functionality into vehicles and its internal electronic architecture. With greater connectivity the number of functions increases, but also the disadvantages in security and thus in safety. Attackers can compromise Electronic Control Units (ECUs) and control the vehicle by injecting packets into the in-vehicle network [Ko10, MV13]. These disadvantages has been demonstrated by the work of Miller and Valasek [MV15]. They showed the first completely remote hack on a Jeep Cherokee, i.e. without having physical access, resulting in a recall of 1.4 million vehicles. Through the Internet-connected head unit of the car, they were able to get access to the Controller Area Network (CAN) and get control over the steering and the engine.

Additional attack surfaces (e.g. WiFi, Bluetooth) were analyzed and exploited by Checkoway *et al.* [Ch11] and Koscher *et al.* [Ko10], resulting in the same conclusion. Attacks on high safety relevant functions are possible in most cases when an attacker can send counterfeit CAN messages from hacked ECUs or additional alien devices. This is possible since CAN

[1] Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany, marcel.kneib@de.bosch.com
[2] Robert Bosch GmbH, Robert-Bosch-Campus 1, 71272 Renningen, Germany, christopher.huth@de.bosch.com

doi:10.18420/in2017_88

is a broadcast bus designed without considering security features [HKD08], allowing all participants broadcast transmission, without any possibility for the receiver to identify the sender. Unfortunately, applying Message Authentication Codes (MACs) or even Digital Signatures in an adequate way, may be infeasible due its extremely limited bandwidth and small payload of 8 bytes per message [LSV12, GM13].

Receiving these counterfeit messages results in critical threats for attached devices and potentially leading to failure of safety relevant functions. Due to high in-vehicular connectivity via distinct buses and gateways, other devices could also be compromised. Gateways are a worthy target for attacks, as they enable message forwarding from a less critical network to a safety relevant network.

To mitigate these vulnerabilities, there are only a few approaches, e.g. using information contained in the transferred signals or to identify the transmitter of received messages. Such techniques allow significant improvements for state-of-the-art Intrusion Detection Systems (IDS) [HKD08, MGF10] and to build secure next-generation CAN gateways verifying the authenticity of forwarded messages [WWP04].

The first technique is to identify transmitters using their clock skew, extracted from periodically occurring messages [CS16]. The idea is that each device is equipped with its own crystal oscillator and these happen to have a skew (e.g. oscillating faster or slower than a reference) with up to 2.4 seconds per day. These skews vary between different ECUs and can be used due to the absence of clock synchronization to distinguish the sender of periodically transmissions.

Another technique is to use the physical properties of the actual signal on the CAN bus, first proposed by Murvay and Groza [MG14]. Here, signals show minor differences in e.g. how quickly a rising edge is set, or how stable a signal is, while being suitable for sender identification. This approach was improved with supervised machine learning algorithms by Choi *et al.* [Ch16] in terms of a better sender classification.

Our contribution is a survey of the two approaches and their evaluation. In addition, we give an outlook on what research is necessary before such systems can be applied to in-vehicle networks.

The remainder of this paper is organized as follows. Section 2 provides information about the Controller Area Network and usage of classical cryptography mechanisms in CAN. In Section 3, the two approaches providing sender identification are described followed by their evaluation in Section 4. The last Section 5 gives a short conclusion and an outlook.

2 Background

2.1 The Controller Area Network

The Controller Area Network is a multicast-based communication protocol, designed in 1983 at Robert Bosch GmbH [Rob91], to replace the expensive and complex wiring scheme in vehicles. One of its main design criteria was to provide a robust transmission. The specification defines data rates from $10\,kbit/s$ to $1\,Mbit/s$. According to the standard, several ECUs are interconnected via two wires, identified as CAN_H and CAN_L, terminated with $120\,\Omega$ resistors. If a recessive bit "1" is present on the bus both wires show the recessive voltage of 2.5 V. When a dominant bit "0" is transmitted the high wire is driven towards 3.5 V and the low wire towards 1.5 V. The differential signal of these two wires represents the transmitted data.

A frame contains a unique 11 bit identifier, representing the frame priority and meaning, and maximal 8 bytes of payload. If a larger identifier is needed, the extended CAN format can be used, thereby increasing the frame by additional 20 bits, two as status bits and 18 bits for the extended identifier.

Since CAN is a multi-master bus each ECU can attempt to access the bus if it is detected idling. In the case of multiple ECUs trying to send their frames simultaneously, the ECU with the highest priority wins the arbitration and can send its frame. Within this arbitration each ECU starts its transmission while it is listening to the bus. If a device recognizes the dominant state while it has transmitted a recessive bit, it will stop immediately. The interrupted device will retry the transmission as soon as the higher prioritized frame was transmitted and the bus is again in idle state.

During the transmission of a frame additional contrary bits, called *stuff buts*, are inserted for synchronization purposes whenever five similar bits are transmitted successively.

2.2 Cryptography in CAN

Existing approaches [GM13, LSV12, VHSV11] try to adopt message authentication on the CAN bus, but it can not be applied easily. This is due to their additionally required resources or their sophisticated modifications.

The approach proposed by Herrewege *et al.* [VHSV11] is to use the CAN+ protocol [ZWT09], an improvement of the CAN protocol. Obviously, it is not practical to apply their approach without making soft- and hardware changes on each ECU.

The authors of [GM13, LSV12] provide message authentication by sending additional messages containing Message Authentication Code (MAC) tags, resulting in a higher bus load and thus to a reduction of available bandwidth. A system with a higher bus utilization

will have weaker communication performance or can be unschedulable. Since CAN is used for critical functions, the reduction of available bandwidth, especially in existing systems, has wide-ranging consequences. The in-vehicle communication systems are well-planned, including defined bandwidth reserves, in order to meet real-time and safety properties. To compensate the higher bus load, a redesign of the whole communication system will be necessary, which will lead to additional buses, a more sophisticated architecture and thus to additional costs. Furthermore, all affected ECUs need more resources to calculate and verify these MACs.

This drawback even holds for the usage of truncated MACs, included in the data field. It is recommended to use at least 64 bits for the MAC tag [Fed16] to ensure sufficient security and collision resistance, which corresponds to the maximum payload. Even if just 24 bits are used, the available payload and thereby the bandwidth will be reduced heavily.

Besides that, MACs do not provide non-repudiation and thus do not protect against counterfeit messages in general, since ECUs capable of verifying these MAC tags are also capable of tampering them. Non-repudiation using cryptographic algorithms can be applied if digital signatures are used. In comparison to MACs they use even more resources and thus are unusable for this purpose.

3 Existing Fingerprinting Approaches

3.1 Clock Skew

Each connected CAN device is equipped with its own quartz crystal clock, which is used to determine the specific moments in time, when periodically sent messages will be transmitted. Concerning distinctions present in these quartz crystals, each independent unsynchronized clock is afflicted with some deviations in comparison to another clock.

Cho *et al.* [CS16] are using these clock skews, to identify the sender of periodically received CAN frames. A periodically occurring message is transmitted every T ms, whereas T_i determines the timestamp of the i-th receiving. The interval ΔT_i between each receiving timestamp consists of $T+\Delta O_i+\Delta d_i$, where d_i denotes the network delay and O_i the difference in time of the transmitting and receiving device. ΔO_i and Δd_i are expected as 0, since the changes of O_i within one step are negligible and periodic CAN frames are constant over time. Thus, the expected timestamp interval can be expressed as $\mu_{\Delta T} = E[T + \Delta O_i + \Delta d_i] \approx T$.

Using the first timestamp and the average of timestamp intervals, $\mu_{\Delta T} \approx T$, the estimated arrival time of the i-th message is $i\mu_{\Delta T} + d_0$. The measured arrival time is $iT + O_i + d_i$. Using these two values, the average difference between the measured and the estimated value, $E[D]$, can be calculated by $E[i(T - \mu_{\Delta T}) + O_i + \Delta d_i] \approx E[O_i]$.

The clock offset $E[O_i]$ is distinct for different transmitters, slowly varying, $E[\Delta O_i] = 0$, and non-zero, $E[O_i] \neq 0$. The slope of the summed accumulated clock offset represents the clock skew, which is constant and thus usable for fingerprinting ECUs.

To recognize intrusions, a linear regression model $O_{acc} = S * t + e$ for a given identifier is determined using the accumulated clock offset, the elapsed time, the previous model and the recursive least squares algorithm. This step is started every N measurements during the operation. A detailed description of the algorithm can be found in [CS16].

The resulting identification error e of the model is then used to identify misbehavior. If no attack is present, the identification error of the model is almost 0, but much higher, if an intrusion is present. This holds, since the clock skew is almost constant and thus the accumulated offset O_{acc} is almost linear in time. Additionally, missing or hijacked messages result in changes of the parameter e, since the resulting accumulated offset does no longer fit the assumed linear model.

3.2 Signal Characteristics

Murvay and Groza [MG14] first mentioned the usability of inconsistencies in the analog signals to identify the sender of a received message. The variations are influenced by production tolerances and therefore are also present if two equal transceivers are used. These variations in the signal characteristic are constant over time, included in each message, caused by immutable physical properties and therefore usable to predict the sender of a message.

For this purpose, Choi *et al.* [Ch16] embed a fixed bit string into the extended identifier field of the CAN frame, which has to be in each message. The receiver of the message samples the signal, concrete the extended identifier, resulting in a variety of analog values. Next, eight time domain and nine frequency domain features are generated using these measurements. Among others, these features are several statistical values, like the mean, standard deviation, lowest and highest value. These 17 features together, extracted from one message, represent a fingerprint, which can be used for sender identification.

To assume the sender of a message, Choi *et al.* [Ch16] use a classification algorithm, which gets trained in a supervised machine learning environment using several previous recorded signals send from each relevant device. A classification algorithm is used to identify the class to which a new observation belongs. Choi *et al.* considered Support Vector Machine (SVM), Neural Network (NN) and Bagged Decision Tree (BDT) in their work. Once a classifier has been trained, it can be used to determine the class an observed fingerprint belongs to.

If a new fingerprint is present, the corresponding identifier is used to decide which device should be predicted by the classification algorithm. If the new fingerprint does not belong to the expected device, an attack is assumed. In this case, there are two different opportunities.

The fingerprint may belong to a known device, to which the identifier of the received message does not belong, indicating a hacked device. Otherwise, if the fingerprint does not belong to any known device, an unknown devices is assumed, what may be caused by an attached alien device.

4 Evaluation

4.1 Clock Skew

Cho *et al.* [CS16] evaluated their approach on a CAN bus prototype and real vehicles using three different attack models. First, the fabrication attack, where an attacker injects an additional forged message from a hacked device while the real device is still sending. As a result, the accumulated clock offset increases at the moment in which the additional message is present, which will also increase the identification error. The second attack model, the suspension attack, occurs when an attacker can persuade a device to stop its transmissions, e.g. by using diagnostic messages. Like in the first attack, the accumulated clock offset and the identification error will increase, due to the absent messages.

The third and most laborious attack is the masquerade attack, a combination of the fabrication and suspension attack. In this scenario, an attacker is able to cause a device to stop the transmission of a particular message and to prompt another device to send the message instead. The changes of the corresponding clock skew is recognizable and additionally a correlation with another clock skew can be used to estimate the origin of the attack.

Cho *et al.* [CS16] evaluated the false alarm rates of their approach using approximately 2.25 million messages recorded in 30 minutes from the real vehicle. Four datasets, containing 300 intrusions, were produced this way. With their clock skew-based approach they were able to detect all anomalies with a false positive rate of 0.055 %. Further improvements, detailed in [CS16], can be used to eliminate all false positives.

4.2 Signal Characteristics

Choi *et al.* [Ch16] evaluated their approach using twelve CAN development boards, where each device produced 900 fingerprints at a baudrate of 500 kBd. The measurements were taken by a 2.5 GS/s oscilloscope and analyzed using MATLAB.

The classification rates, which are used to predict the belonging of a fingerprint vary between 83 % and 100 %, whereby the highest misclassification rate is 13.22 % for the SVM, 14.44 % for the NN with 100 hidden nodes and 14.22 % for the BDT with 100 classifiers. These rates are obviously only available for known devices. Unknown devices are assumed if all classification rates for a given fingerprint are below some threshold. Identifying unknown devices works for SVM with an Equal Error Rate (EER) of 0 and for the BDT with an ERR of 0.005.

4.3 Comparison

The biggest limitation of the clock skew approach is its inability of monitoring aperiodic messages, since the clock skew is extracted from periodic occurring messages. For the same reason, it is only possible to identify the device on which the attack is mounted if the intrusion can be observed for a longer time. Further, the linear model is always updated after N measurements. If the number of needed measurements is too large, an attacker may reach his goal before the intrusion is detected.

The limitations of the approach using signal characteristics are the extended frame format, since it increases the bus load, what may has wide ranging consequences as mentioned in Section 2.2. Furthermore, each device needs a software update to implement the extended identifier, which is only possible if it is not used for its original purpose. Besides that, the variations of the signal characteristics are contained in the whole frame, not just in the extended identifier field. For this reason, these information should be used instead of an additional special purpose field.

5 Conclusion

Fingerprinting ECUs on CAN could improve the security of in-vehicle networks significantly, since attacks on vehicles are often only possible as an attacker gets access to the internal vehicle communication. Especially for the Controller Area Network, these technologies constitute a promising opportunity to increase its security and thus safety, since adding classical cryptographic mechanisms is only limited applicable.

Both approaches have its advantages and disadvantages. The clock skew-based approach does not need special hardware nor software modifications, but is only usable for periodic messages. The approach using signal characteristics is applicable for both, aperiodic and periodic messages, but needs expensive hardware extensions for measurements.

As a general result, fingerprinting ECUs promise an interesting method of identifying the sender of in-vehicle messages. For both approaches more research is necessary before it is suitable for safety critical systems. It must be clarified how reliable both approaches are, especially how difficult it is to circumvent the clock-based approach. For the signal characteristic-based approach, it is necessary to test the operational capability in a real vehicle and to find a way to use the normal CAN frame instead of an additional fixed bit string.

References

[Ch11] Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T.: Comprehensive Experimental Analyses of

Automotive Attack Surfaces. In: Proceedings of the 20th USENIX Conference on Security. SEC'11, USENIX Association, Berkeley, CA, USA, pp. 6–6, 2011.

[Ch16] Choi, W.; Jo, H. J.; Woo, S.; Chun, J. Y.; Park, J.; Lee, D. H.: Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. CoRR, abs/1607.00497, 2016.

[CS16] Cho, K.; Shin, K. G.: Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. In: 25th USENIX Security Symposium (USENIX Security 16). USENIX Association, Austin, TX, pp. 911–927, 2016.

[Fed16] Federal Office for Information Security. TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths, October 2016.

[GM13] Groza, B.; Murvay, S.: Efficient Protocols for Secure Broadcast in Controller Area Networks. IEEE Transactions on Industrial Informatics, 9(4):2034–2042, Nov 2013.

[HKD08] Hoppe, T.; Kiltz, S.; Dittmann, J.: Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures. In: Computer Safety, Reliability, and Security: 27th International Conference. Springer Berlin Heidelberg, pp. 235–248, 2008.

[Ko10] Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.: Experimental Security Analysis of a Modern Automobile. In: 2010 IEEE Symposium on Security and Privacy. pp. 447–462, May 2010.

[LSV12] Lin, C. W.; Sangiovanni-Vincentelli, A.: Cyber-Security for the CAN Communication Protocol. In: 2012 International Conference on Cyber Security. pp. 1–7, Dec 2012.

[MG14] Murvay, P. S.; Groza, B.: Source Identification Using Signal Characteristics in Controller Area Networks. IEEE Signal Processing Letters, 21(4):395–399, April 2014.

[MGF10] Müter, M.; Groll, A.; Freiling, F. C.: A structured approach to anomaly detection for in-vehicle networks. In: 2010 Sixth International Conference on Information Assurance and Security. pp. 92–98, Aug 2010.

[MV13] Miller, C.; Valasek, C.: Adventures in Automotive Networks and Control Units. In: Defcon 21. 2013.

[MV15] Miller, C.; Valasek, C.: Remote Exploitation of an Unaltered Passenger Vehicle. In: Defcon 23. 2015.

[Rob91] Robert Bosch GmbH. CAN Specification v2.0, 1991.

[VHSV11] Van Herrewege, A.; Singelee, D.; Verbauwhede, I.: CANAuth - A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus. In: ECRYPT Workshop on Lightweight Cryptography 2011. 2011.

[WWP04] Wolf, M.; Weimerskirch, A.; Paar, C.: Security in automotive bus systems. In: Workshop on Embedded Security in Cars. 2004.

[ZWT09] Ziermann, T.; Wildermann, S.; Teich, J.: CAN+: A new backward-compatible CAN protocol with up to 16× higher data rates. In: Design, Automation & Test in Europe Conference & Exhibition, 2009. DATE'09. IEEE, pp. 1088–1093, 2009.