Securing Tire Pressure Monitoring System for Vehicular Privacy

Mark Vaszary Andreas Slovacek Yanyan Zhuang Sang-Yoon Chang
Department of Computer Science
University of Colorado Colorado Springs
{mvaszary, aslovace, yzhuang, schang2}@uccs.edu

2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) | 978-1-7281-9794-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCNC49032.2021.9369576

***Abstract*—Modern vehicles are equipped with vehicular sensors for smart navigation, vehicle state awareness, and other intelligent operations. Despite the previous belief that the sensor operations stay within a vehicle, as it is designed to be, we study information leakage through the tire pressure monitoring system (TPMS) sensors and the corresponding privacy breach. We demonstrate that, using a low-cost and off-the-shelf software defined radio (SDR), an unauthorized attacker can track uniquely-identifiable sensor IDs up to 40 meters away from the vehicle. To address the issue and protect vehicular privacy, we also propose an effective and lightweight TPMS ID randomization scheme and analyze its security and the implementation costs.**

I. Introduction

Vehicles are becoming increasingly intelligent and have reached the point of having fully-automated and self-driving prototypes operating on the roads. Such modern vehicles are equipped with *vehicular sensors* to collect and observe new information and *vehicular networking*[1] with the radios to exchange information with other vehicles or traffic infrastructure. Although vehicular sensors use wired networking for intra-vehicle communications through controller area network (CAN bus), such vehicular sensor networking is distinguishable from the wireless-communication-based vehicular networking designed for communicating with an external entity, since the CAN-bus-based sensor networking is designed to stay within a vehicle between the electronic control units (ECU) and the embedded sensors.

Vehicular privacy to prevent an unauthorized attacker from tracking the behavior and the location of a vehicle has emerged as a critical challenge for wireless-based vehicular networking. For example, Security Credential Management System (SCMS) is driven by the US government and the Crash Avoidance Metrics Partnership (CAMP), including the major international car companies, and presents one of the most advanced and complex public-key infrastructure (PKI) designs incorporating both pseudonym-based and dynamic credentials and multiple authorities for the vehicular PKI. To preserve the vehicular privacy in vehicular networking remains an active research challenge.

Despite the active research and development on privacy in vehicular networking, such advancements are significantly lacking in the field of vehicular sensors. Since vehicular sensors are designed for vehicle-internal purposes, it has been widely believed that an unauthorized attacker has to physically compromise the vehicle for accessing the sensor operations and networking. The sensor-based vehicular privacy breach requiring physical compromise of the vehicle therefore has generally believed to have a low threat feasibility, and therefore low security risk, especially compared to the remote threat model for vehicular networking or vehicular ad hoc networking (VANET).

We challenge the belief that vehicular sensor networking (the networking of the vehicular sensors within a vehicle, as opposed to VANET) is contained within a vehicle and demonstrate that a remote attacker can compromise the sensor-networking signals despite its design to be used within the vehicle. More specifically, we focus on the TPMS, which is the only intra-vehicular sensor relying on wireless communications to connect to the CAN bus due to the physical motions of the vehicle wheels. TPMS is widely used in modern vehicles since it has been factory-mandated in 2008 in the US and in 2012 in Europe. 104 Million vehicles or at least 70% of the registered vehicles are estimated to be equipped with TPMS in the US [1]. Other short range communications, such as key fob, are not designed for real-time sensor updates to the vehicle.

In this paper, we address the issue of information leakage caused by TPMS sensors, which undermines the extensive and ongoing privacy research in the vehicular networking field. For example, even if the privacy protection is in place for vehicular networking, the leakage caused by TPMS sensors can be used to breach the privacy and enable an unauthorized attacker to track the behaviors and whereabouts of a vehicle. This issue is insufficiently addressed in the previous research, despite the earlier discovery of such a threat [2] (we discuss the previous research in Section III). Our work demonstrates that this problem still persists and is pervasive in modern vehicles. Our work also demonstrates that the threat barrier got significantly lower since the earlier proof-of-concept discovery due to the advancement in wireless radio technology, including software-defined radios (SDR). The security/privacy risk got higher because SDR radios are readily available at low costs and enables the privacy attack prototyping with software control and programming (as opposed to the radio engineering expertise).

The privacy risk is pervasive as TPMS is standardized and

[1]The vehicular networking is also called vehicular ad hoc networking (VANET) as well as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or generally vehicle-to-everything (V2X) communications.

general across the vehicle models. In addition to experimenting on three distinct vehicles we own (all of which were manufactured after the aforementioned threat discovery by security research) as a proof of concept and for threat performance measurements, we observe the vulnerability in the real world as we passively monitor the streets and highways with our attack implementation; the cars on the roads are vulnerable and leaking the TPMS signals for privacy breach. Our attack implementation is described in Section IV-B and its performance measurements for capturing the TPMS signals are in Section IV-C.

We address vehicular privacy but focus on sensor networking designed for intra-vehicle operations, as opposed to the vehicular communications for external networking. Our work also focuses on vehicular privacy as opposed to the TPMS data confidentiality, because the TPMS message confidentiality is of relatively low security risk in its application as described in Section II. The vehicular privacy leakage for our work is actually from the TPMS message headers including the TPMS ID, unique to a vehicle.

We make two key contributions to protect vehicular privacy in vehicular sensor networking. First, we demonstrate that the vulnerability still widely exists and poses an even greater risk, due to the radio technology advancement and accessibility, to raise awareness of this important privacy vulnerability and threat. Second, to address the privacy threat, we build an efficient/lightweight and effective countermeasure to defend against such threat based on randomizing the TPMS identifier.

II. Background

Vehicular Sensors. A modern vehicle has many sensors distributed throughout the vehicle. These sensors connect to the vehicle's ECUs and send messages that the vehicle either takes action on, or displays to the vehicle's driver. There are sensors for monitoring temperature through the critical components of the vehicle (e.g. powertrain, drivetrain), as well as the climate control for the vehicle cabin. Other sensors exist to assist with steering, acceleration and braking functions, critical for the driver assisted operation of the vehicle. With the number of vehicle automation features increasing each year, the total number of sensors is also increasing, as vehicles quickly become more autonomous and closer to achieving Level 5 capability for self-driving [3].

TPMS System. TPMS is used within vehicles to monitor the state of each tire. A vehicle has four tires each with a TPMS sensor. Each TPMS sensor transmits its packet wirelessly; the vehicle has a designated receiver for these packets, which are then sent to an ECU by wire. TPMS sensors communicate one-way: they send a variety of information, such as tire pressure and temperature. The TPMS system is generic across the vehicle models and is standardized across nine different protocols in the communication data formats and the two broadcasting frequencies.

Intra-Vehicular Communications. Intra-vehicular communications consist of wired communications through the CAN bus, and wireless communications that are received through the vehicle's receiver. Space comes at a premium and wireless transmissions offer savings in space and material. Currently there are two subsystems that utilize the wireless receiver: key FOBs to access and start the vehicle, and TPMS. The vehicle's receiver receives TPMS sensor broadcasts and processes those signals to the vehicle's ECU through the CAN bus.

The vehicle's receiver only listens for those TPMS sensor IDs that are learned or linked to that receiver; any other IDs are ignored and not processed. TPMS received messages are typically displayed in the vehicle's instrument panel presented to the driver in real time.

The TPMS system has unique sensor communication channel in that it is wireless (unlike other vehicular sensor communications using wired connections via CAN bus, except for the keyless entry system) and in that the wireless communication is in plaintext without cryptographic processing (unlike the keyless entry system). The TPMS communication forgoes cryptographic processing because the TPMS message is not confidentiality-sensitive and is of low security risk, i.e., the impact of the attacker knowing the TPMS message values has low security impact. Our work therefore does not aim to protect message confidentiality but rather focus on the vehicular privacy.

III. Related Work

Vehicular Privacy. Vehicular privacy is to prevent unauthorized attackers from tracking the whereabouts or learning the operations of vehicles. Prior research to achieve vehicular privacy focus on the vulnerabilities and threats from vehicular networking (VANET) [4]–[9] For example, vehicular networking introduces a credential management system and a public-key infrastructure (PKI), which is significantly more advanced than the PKI designs/systems in other applications to support vehicular privacy and uses pseudonym-based and dynamic certificates for establishing the root of trust for vehicular networking [5]–[7]. Our work is distinguishable from that body of vehicular privacy research since our focus is on TPMS designed for intra-vehicle communication.

Security in Vehicular Sensor and Control. Previous research demonstrated that the vehicle control, and the CAN bus used for internal networking, are vulnerable to compromise and threats; in addition to the threat using the physical interface to the CAN bus, they investigated the remote threats which do not have the physical access to the vehicle [2], [10], [11], including using the Internet channel originally designed for updating the entertainment system as the initial breach point to the CAN bus [10], [11]. These works provided a comprehensive treatment of the threats on intra-vehicular networking and control, including those threatening integrity (the malicious attacker attempting to control or influence the vehicle operations). Our work has a sharper focus on vehicular privacy than these work.

Particularly relevant to our work are the prior research focusing on TPMS. TPMS has vulnerabilities that include battery drain of the vehicle's primary 12V battery as well as the tire sensor batteries [12], [13], replay and spoofed

5 bits	28 bits	8 bits	8 bits	8 bits	8 bits
Preamble	**Sensor ID**	**Pressure**	**Temperature**	**Flags**	**CRC**

Fig. 1: TPMS data payload format.

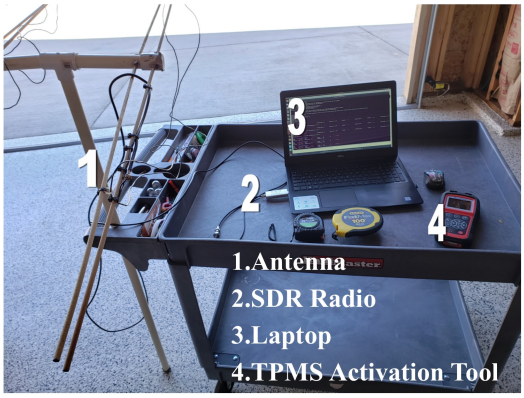


Fig. 2: Hardware equipment for our threat implementation.

TPMS messages, and the injection of malicious messages that can immobilize or confuse the receiver ECU [2]. Our work corroborates with the vehicular privacy issue findings from Rouf et al. [2]. However, when investigating the privacy threat, we distinguish our work from Rouf et al. [2] in two ways. First, we implement the threat with significantly lower cost due to the technological advancement in SDR; our equipment costs less than $50 (with the radio costing $30) in contrast to $1500 for Rouf et al. [2], significantly increasing the threat feasibility and thus the security risk. Second, we provide more detailed analyses of the wireless signals getting leaked, including the analog-domain SNR measurements at various distances and angles. In addition, we propose a countermeasure to address the privacy vulnerability.

Recent work in securing TPMS communication has proposed workarounds such as decreasing the required signal strength of TPMS sensors [14], encrypting the entire TPMS message [15], and so on. Our work, however, prioritizes efficiency over confidentiality and encryption of the entire message, which require additional decryption in comparison.

IV. The Threat: TPMS Signal Leakage

We investigate the threat of using the TPMS signal leakage to breach vehicular privacy. The vulnerability arises because the TPMS messages are wirelessly broadcasted in cleartext. More specifically, the message is wirelessly propagated outside of the vehicle, lacking encryption protection. Therefore, any eavesdropper can track TPMS sensor messages and IDs, and hence the vehicle's whereabouts and behaviors.

Our results demonstrate that the privacy concern established by Rouf et al. [2] still exists. More concerning, the technology threatening privacy is exponentially more accessible. First, the threat based on TPMS signal leakage is generally applicable across vehicle makes/models and the TPMS sensor vendors, as we describe in Section I. Second, we did not encounter any TPMS with adequate protection for vehicular privacy. In addition to the opportunistic eavesdropping on streets and highways, the three vehicles on which we primarily tested our attack implementation are distinct in makes and models; the model years being (2019, 2015, and 2013). Because threat demonstration is generally applicable, we obfuscate the specific make/model of the vehicle used for our experiment in Section IV-C.

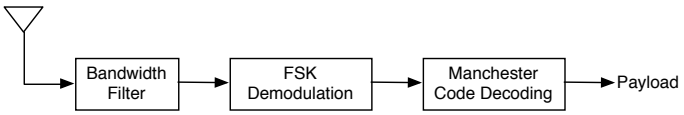


Fig. 3: Attacker's processing chain at the physical layer.

A. Threat Model

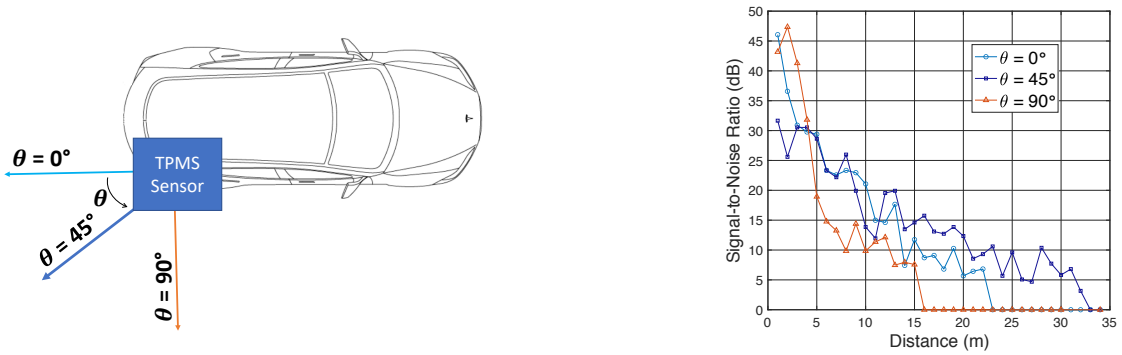
We consider a passive attacker who remotely eavesdrops on the sensor networking. More specifically, the attacker eavesdrops on the networking between the TPMS sensor and the corresponding receiver on board in the vehicle. The attacker is *remote* in that they do not require the physical access of the vehicle nor the compromise of the subsystems of the vehicle. We consider a remote attacker since it increases the attack feasibility, and thus increases the security risk compared to that requiring the physical access or compromise. Any attacker equipped with the radio hardware and capabilities can launch the attack described in this section. We also consider an attacker capable of continuously monitoring/eavesdropping and capturing consecutive TPMS transmissions, e.g., near the vehicle across the TPMS transmissions.

While we focus on vehicular privacy, we do not consider the threats against the message confidentiality of the TPMS message for the following two reasons. First, the payload does not contain confidentiality-sensitive information except for the sensor ID (which we randomize in our work) as seen in Figure 1. Second, we prioritize efficiency for our defense design because of the embedded nature of our vehicular application with power constraints. Furthermore, additional side channels, such as those based on RF signals [16], to track the vehicle are outside the scope of this work, as we focus on digital information-based tracking.

B. TPMS Eavesdropping Attack Implementation

We build a prototype for the attacker using: a SDR (RTL-SDR), a home-made antenna, and a Ubuntu laptop to process the signals from the SDR (equipped with RTL_433 and GNU-Radio Companion, or GRC). The hardware equipment for our attacker implementation is shown in Figure 2. The cost of the hardware equipment, excluding the laptop and the TPMS activation tool, is less than $50.

In signal processing, the attacker processes the received signal through a filter to limit the noise (100 kHz bandwidth centered at 433 MHz), the binary frequency-shift-keying (binary FSK) demodulation, and a decoding module based on Manchester Coding. Figure 3 describes the physical-layer processing on the eavesdropping attacker. The output yields the TPMS message, depicted in Figure 1.



(a) Measuring TPMS sensor signal leakage to vehicle receiver.

(b) SNR over distance from various angles (θ). Discrete data measurements are in markers and measured every one meter.

Fig. 4: Measurement of TPMS sensor signal leakage.

C. Experiment for Attack Performance

We focus on the attack performance experiment in this section. To carry out the attack, we measured the distance from the tire sensor at which both the analog and digital signals could be decoded. By measuring both the analog and digital signals, we can see how the signal attenuates from the tire sensor, and how far away one can effectively perform an eavesdropping attack on the broadcast signal.

For greater control in the experiment (enabling attacker receiver capture beyond just opportunistic TPMS transmissions), we used the TPMS activation tool (depicted in Figure 2) to actively probe and trigger the TPMS sensor message. Furthermore, we limited the natural noise negatively affecting our measurements by experimenting in a large and empty parking lot (free from other 433 MHz signals, such as weather monitoring stations etc.) and by experimenting on a day free from rain, fog, and snow (limiting the weather interference with the RF transmission from the TPMS).

We measure the signal attenuation performance in the digital domain (signal-to-noise ratio, or SNR, after the Filter in Figure 3) as well as in the analog domain (the decodability measured after the the Manchester decoding in Figure 3). We measure attenuation of the TPMS sensor signal strength over three different angles (θ), with varying distance from the tire, as shown in Figure 4(a). θ = 0° measured the signal leakage in the same parallel direction away from the vehicle, as the attacker could either be following behind the vehicle or ahead in front of it if tracking the closest tire. θ = 45° was measured at 45 degrees from the vehicle tire, assuming that the attacker was trailing behind the target vehicle in the blind spot area. θ = 90° was measured perpendicular to the vehicle tire, when the attacker is travelling next to the target vehicle or more than one lane across from it.

Our analog SNR measurement results are shown in Figure 4(b). The signal attenuates rapidly in dB as the distance increases. In fact, after 16m, after 23m, and after 33m for $\theta = 90°$, $\theta = 0°$, and $\theta = 45°$, respectively, the signal power becomes even smaller than the noise power. The $\theta = 45°$ direction outperforms other angles because of the TPMS sensor antenna orientation.

We also measure the digital decodability to learn how far the attacker can be from the vehicle to decode the TPMS message. Even when the noise power dominates the signal power and has greater magnitude (e.g., after 34m for $\theta = 45°$), we are still able to decode the digital signal. More specifically, at θ = 0° direction, we are able to digitally decode the signal up to 27 meters, and for other directions, we are able to decode the signal at 35 meters or longer.

Our work corroborates with [2] with comparable distance measurements for decodability. However, we provide more detailed analysis with the physical-layer metric of SNR and experiment on the recent vehicles manufactured after the threat discovery [2]. Thus the threat is still pervasive as of 2020.

V. The Defense: TPMS ID Randomization

Our defense is based on dynamically varying and randomizing the TPMS ID and therefore preventing an eavesdropping attacker from tracking the vehicle. Both the TPMS sensor and the vehicle-on-board receiver update the ID for every transmission. While randomization techniques have also been used for availability purposes in the form of moving target defense varying the identifiers [17], [18] and other control communication parameters (e.g., spread spectrum for anti jamming), we use the randomization to prevent the unauthorized vehicular tracking by using random ID's in the communications.

We design our defense to randomize the TPMS ID only, as opposed to encrypting the entire message, because we prioritize efficiency over confidentiality of the entire message. More specifically, our approach does not encrypt the TPMS communication so that the randomization verification involves a simple comparison rather than the decryption processing. Because updating the ID is critical for our scheme, in this section, we contrast a simple increment-based *Naive* scheme with *random* scheme (Section V-A) and then analyze the security costs of implementing such schemes (Section V-D).

A. Random Update (vs. Naive Update)

Naive update increments the TPMS ID to dynamically vary the ID, since static ID provides the tracking/linkage vulnerability between distinct transmissions. However, while effective against sporadic attacker, such Naive scheme is vulnerable

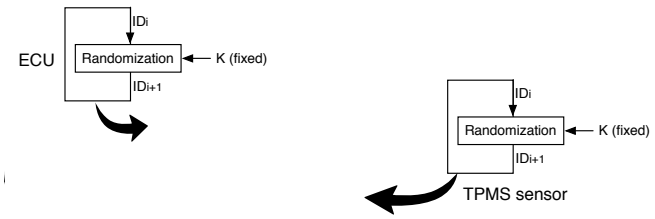


Fig. 5: TPMS ID Randomization

against an attacker capable of monitoring the TPMS transmissions continuously and capturing consecutive transmissions (as described in Section IV-A). Because of the dependency between IDs (the impending ID is simply one greater than the current), the attacker can still track the vehicle.

To provide independence across the ID updates to prevent the attacker from tracking the ID, we design and implement a *random* scheme. The randomization updates are based on a pseudo-random generator using a lightweight block cipher with cipher block chaining (CBC) mode with no new input plaintexts. In other words, the random output from the Randomization algorithm (providing the current ID) becomes the input of the algorithm for the next ID update. Figure 5 depicts our randomization scheme. Using a Randomization algorithm, the output corresponds to the randomized ID for the TPMS communication header (ID_i) where i corresponds to the TPMS transmission time index. This output then becomes the input for the next communication. At time $i+1$, ID_i is the input of the Randomization algorithm, i.e., $ID_{i+1} = \text{Randomization}(K, ID_i)$. The seed/key K for driving the pseudo-random generator Randomization is fixed, and is generated when the TPMS sensor is deployed on the vehicle, e.g., the tire gets replaced.

B. Security Analyses

We apply well-established cryptographic primitives for the security of our randomization scheme. We require the Randomization algorithm to 1) produce pseudo-random outputs, e.g., tested by National Institute of Standards and Technology (NIST), 2) exhibit the Avalanche effect (one bit change in the input changes about the half of the bits in the output in order to defeat differential cryptanalysis), and 3) protect the secrecy of K even when the Randomization output ID is known (known as the Confusion property in security). There are fortunately many cryptographic algorithms satisfying these requirements. For Randomization, we focus on two algorithms – Advanced Encryption Standard (AES) [19] and Lightweight Encryption Algorithm (LEA) [20], [21] – with the shortest key length of 128 bits because of their efficiency. AES and LEA are even used in the body area network [21], [22] whose networks are comprised of sensor devices with even greater resource constraints. We further study their efficiency and implementation costs in Section V-D. AES and LEA are also appropriate for Randomization because they process in block lengths of 128 bits (corresponding to the output length) and therefore provide sufficient bits/entropy for the TPMS ID, which can be up to 9 Bytes or 72 bits at the maximum; we use the least significant bits equal to the length of our implementation.

We also rely on the secrecy of the seed K for Randomization. We assume that there is no privacy threat at the bootstrapping of the tire, when K is generated. After the generation and bootstrapping, K does not leave the local devices of the TPMS sensor and the ECU receiver; its security is as reliable as the private keys in public-key cryptography, as the private keys also do not leave the owner device once generated. Due to the aforementioned requirement for the Randomization algorithm, given ID_i for any i (for example, an attacker eavesdrops on the communication and learns ID_i), it is computationally infeasible to derive K. However, given K and ID_i (which is the case for the authorized TPMS sender and on-board ECU receiver), it is easy and efficient to generate ID_{i+1}. K therefore also serves as a cryptographic salt because the attacker knowing ID_i at communication i cannot compute the ID of the next communication (ID_{i+1}) without K.

C. Synchronization

For the ID-update synchronization, both the TPMS transmitter and ECU receiver update the ID for every transmission. The TPMS transmitter and the ECU receiver locally compute the randomization separately, as described in Figure 5, and use the randomized ID ID_i for secure communications preserving vehicular privacy. In addition, for automatic synchronization of i, the ECU receiver tries and accepts a window of IDs after the last verified ID, in the case when the wireless transmission packets get lost and the TPMS and ECU are off in their randomization counts. In other words, even if a transmission gets lost, the ECU receiver can automatically synchronize to and use the latest ID, while dropping the previous IDs corresponding to the lost transmissions. In our experiments, one TPMS message (e.g., indicating tire pressure low) triggers repeated transmissions (greater than 5 repeated transmissions, depending on the vehicle and TPMS sensor model) for redundancy and better control of such error in transmission. Such synchronization requires no extra communication overhead. Efficient and automatic synchronization is also enabled by the one-way nature of TPMS communication, i.e., TPMS sensor communicates to the ECU receiver but the ECU does not transmit back to the TPMS sensor.

D. Security Cost Analyses

We compare the security costs of using AES vs. LEA for the ID randomization; these algorithms are appropriate for our secure randomization scheme as explained in Section V-B. Our cost analyses include execution time, processing usage, and memory. For our experimental setup, we use a power, memory and storage constrained device, Raspberry Pi model 2B, to demonstrate the efficacy of potential cryptographic solutions for privacy on an embedded-friendly platform. Raspberry Pi model 2B has a Broadcom BCM2835 SoC, 512 RAM, and was overclocked to 900MHz. We implemented AES-128 and LEA-128 using the C++ CryptoPP libraries. For power measurements, a J7-C USB tester was used to measure changes in watts, volts and energy (in terms of watt-hours);

	AES	LEA
Code Size (KB)	300	413
Clock Cycles per Byte	68	182
Power Consumption (watts)	1.405	1.405
%CPU Usage	20.9	20

TABLE I: Security Cost Measurements for Randomization

the measurements are kept to significant digits with limited fluctuations in the values.

The experimental results are summarized in Table I. Comparing AES-128 and LEA-128, AES is superior to LEA in code storage and execution time while having comparable power consumption and CPU usage. AES has a smaller code size (300KB vs. 413KB), and AES' execution-time-per-update is shorter than LEA by $\frac{68}{182} = 0.374$ clock cycles per byte. From our measurements in Table I, we also derive the execution time (1.209μs for AES vs. 3.236μs for LEA). We recommend using AES for our ID-randomization defense because its security cost performance exceeds LEA (this section) and has stronger security properties than the Naive scheme (Section V-A).

VI. Conclusion

In this work, we demonstrate that uniquely-identifiable TPMS sensor communications can be tracked up to 40 meters away from the vehicle, making it vulnerable against vehicular privacy. We show that the vulnerability not only exists as of today, but its security risk increased significantly, due to the advancement in radio technology and the wider availability of SDR at an attacker's disposal. We propose a TPMS ID randomization scheme to secure the TPMS sensor communications and protect vehicular privacy. We analyze our randomization scheme's security to study its effectiveness and analyze the implementation costs using a prototype to facilitate its practical deployment.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1922410. This research is also supported in part by Colorado State Bill 18-086. We would also like to thank the anonymous reviewers for their helpful feedback.

References

[1] "Global adoption of tpms." [Online]. Available: https://www.schradertpms.com/en/driver-education/global-adoption-tpms

[2] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proceedings of the 19th USENIX Conference on Security*, ser. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 21–21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929848

[3] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Vehicle as a Mobile Sensor," *Procedia Computer Science*, vol. 34, pp. 286–295, Jan. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050914008801

[4] R. Lu, X. Lin, H. Zhu, P. . Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, April 2008, pp. 1229–1237.

[5] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, Dec 2018.

[6] C. Chen, S. Chang, Y. Hu, and Y. Chen, "Protecting vehicular networks privacy in the presence of a single adversarial authority," in *2017 IEEE Conference on Communications and Network Security (CNS)*, Oct 2017, pp. 1–9.

[7] J. Brorsson, P. S. Wagner, and M. Hell, "Guarding the guards: Accountable authorities in vanets," in *2018 IEEE Vehicular Networking Conference (VNC)*, Dec 2018, pp. 1–4.

[8] J. Song, Y. Zhuang, J. Pan, and L. Cai, "Certificateless secure upload for drive-thru internet," in *2011 IEEE International Conference on Communications (ICC)*. IEEE, 2011, pp. 1–6.

[9] D. Eckhoff and C. Sommer, "Driving for big data? privacy concerns in vehicular networking," *IEEE Security Privacy*, vol. 12, no. 1, pp. 77–79, 2014.

[10] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*, May 2010, pp. 447–462.

[11] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Conference on Security*, ser. SEC'11. Berkeley, CA, USA: USENIX Association, 2011, pp. 6–6. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028067.2028073

[12] S.-Y. Chang, S. L. S. Kumar, B. A. N. Tran, S. Viswanathan, Y. Park, and Y.-C. Hu, "Power-positive networking using wireless charging: Protecting energy against battery exhaustion attacks," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '17. New York, NY, USA: ACM, 2017, pp. 52–57. [Online]. Available: http://doi.acm.org/10.1145/3098243.3098265

[13] V. Desnitsky, N. Rudavin, and I. Kotenko, "Modeling and evaluation of battery depletion attacks on unmanned aerial vehicles in crisis management systems," in *Intelligent Distributed Computing XIII*, I. Kotenko, C. Badica, V. Desnitsky, D. El Baz, and M. Ivanovic, Eds. Cham: Springer International Publishing, 2020, pp. 323–332.

[14] A. Kolodgie, P. Berges, R. Burrow, M. Carman, J. Collins, S. Bair, G. D. Moy, J. M. Ernst, and A. J. Michaels, "Enhanced tpms security through acceleration timed transmissions," in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017, pp. 35–39.

[15] D. K. Kilcoyne, S. Bendelac, J. M. Ernst, and A. J. Michaels, "Tire pressure monitoring system encryption to improve vehicular security," in *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE, 2016, pp. 1219–1224.

[16] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 116–127. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409959

[17] Y. Zhou, G. Cheng, S. Jiang, Y. Hu, Y. Zhao, and Z. Chen, "A cost-effective shuffling method against ddos attacks using moving target defense," in *Proceedings of the 6th ACM Workshop on Moving Target Defense*, ser. MTD'19. New York, NY, USA: Association for Computing Machinery, 2019, p. 57–66. [Online]. Available: https://doi.org/10.1145/3338468.3356824

[18] S. Chang, Y. Park, and B. B. Ashok Babu, "Fast ip hopping randomization to secure hop-by-hop access in sdn," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 308–320, 2019.

[19] J. Daemen and V. Rijmen, "Aes proposal: Rijndael (1999)," 1998.

[20] D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, and D.-G. Lee, "Lea: A 128-bit block cipher for fast encryption on common processors," in *International Workshop on Information Security Applications*. Springer, 2013, pp. 3–27.

[21] A. Z. Alshamsi and E. S. Barka, "Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks," in *2017 International Conference on Informatics, Health & Technology (ICIHT)*. IEEE, 2017, pp. 1–7.

[22] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. Kwak, "A comprehensive survey of wireless body area networks," *Journal of medical systems*, vol. 36, pp. 1065–94, 08 2010.