Feasibility of Verify-on-Demand in VANETs

Sebastian Bittl
Independent
Munich, Germany
sebastian.bittl@mytum.de

Karsten Roscher
Fraunhofer ESK
Munich, Germany
karsten.roscher@esk.fraunhofer.de

***Abstract*—Wireless ad hoc networks are an important topic in the automotive domain. Thereby, strict security requirements lead to high effort for verification of digital signatures used to secure message exchange. A popular approach to limit such effort is to apply verify-on-demand schemes. However, we show that verify-on-demand requires much more cross layer dependencies than identified before. Moreover, a massive denial of service weakness of this kind of verification mechanism is found. Thus, we recommend to prefer verify-all schemes over their verify-on-demand counterparts.**

***Index Terms*—Verify-on-Demand, VANET, Security;**

I. Introduction

Vehicular ad hoc networks (VANETs) are a topic of high interest, as they promise to increase future safety of driving. Wireless data exchange and realtime requirements of safety critical use cases require strong but yet efficient security mechanisms for VANETs. This even holds for the so called Day 1 use cases, for which mass deployment is planned within upcoming years [1]–[3].

To provide authenticity and integrity of exchanged messages, these are typically signed using primitives of asymmetric cryptography and elliptic curve cryptography (ECC). However, high numbers of received broadcast messages pose performance problems for signature verification at receivers. Realization of hardware verification modules capable of verifying all received messages under high node density is still challenging [4], [5]. Thus, mechanisms for reducing the number of required verifications have been looked at.

Verify-on-demand (VoD) performs a relevance check for the message, which is only verified after is was identified to be relevant, i.e., its contained information is to be used by the receiver. [6] suggests to derive the relevance check directly from the decision making process of applications. This is based on the design of the US WAVE (Wireless Access in Vehicular Environments) standardization framework and extension of this scheme to the ETSI ITS (Intelligent Transport System) standards has not been looked at in detail [7]. Moreover, it is assumed that a relevance decision only affects a single message [6].

We show that the need for authenticated data sets does not only arise from within the application layer, but also from other protocol layers. Moreover, introduction of VoD leads to a complex set of dependencies between functionality on different protocol layers. Furthermore, we find that introduction of VoD significantly decreases the burden for an attacker to perform a denial of service (DOS) attack on a VANET. Additionally, the discovered DOS weakness can be well targeted to dedicated nodes without significant influence on other nodes, which differentiates the attack from other common DOS attacks in VANETs.

Related work is looked at in Section II. General security considerations about VoD are given in Section III. Sections IV and V study cross influence between VoD and routing functionality as well as certificate handling, respectively. Afterwards, Section VI proposes a dedicated DOS attack on VoD. Finally, Section VII provides a conclusion about this work.

II. Related Work and Attacker Model

The VoD concept is introduced in [6] as an alternative to a verify-all scheme. Thereby, a verify-all scheme is characterized by verification of all received messages before these are handed over to further message parsing. In contrast, VoD only verifies messages after a demand for usage of their content has been identified. The impact of VoD on overall security in VANETs is only studied very briefly in [6]. Some background about the VoD concept is given in [7].

VoD was initially proposed for WAVE, i.e., in connection with information dissemination via BSMs (basic safety messages). In contrast, ETSI ITS uses CAMs (cooperative awareness messages) for cyclic data distribution as well as DENMs (decentralized environment notification messages) for on demand information dissemination [3]. Moreover, WAVE does not describe a way to store the content of received messages, while ETSI ITS uses an LDM (local dynamic map) to store dedicated VANET messages.

[8] proposes an implementation of the VoD concept for ETSI ITS by storing signatures alongside with corresponding messages in an extended LDM. Moreover, the LDM also hands over messages to the security entity for verification and stores the corresponding result to avoid multiple verification of a single message. However, our analysis in Section IV shows that this approach leads to massive cross layer dependencies.

Dedicated network layer protocols for VANETs have been developed. Thereby, a major difference between WAVE and ETSI ITS is the support for multi-hop communication, which is only available in ETSI ITS. Within ETSI ITS the term GeoNetworking is commonly used, as network layer routing in VANETs is often based on geographic properties of the vehicular environment. Two major concepts for forwarder selection exit. Firstly, the sender of a message can select the next hop, e.g., by greedy forwarding [9]. Secondly, the sender can be selected in a decentralized manner, e.g., by contention

based forwarding (CBF) [10]. The influence of VoD on multi-hop communication has not been regarded in prior work.

DOS attacks on VANETs are a well known issue. Typically, jamming or misuse of certificate dissemination features is used to raise the channel load in a dedicated area in a way to cause ordinary communication to become at least unreliable or even brake down completely [11], [12]. [6] argues that DOS attack surfaces of the VoD scheme do not increase the vulnerability of the VANET, as VANET security could be always attacked by this kind of attacks. In contrast, we show that VoD significantly reduces the burdens of an attacker to perform a DOS attack. Moreover, the attacker does not even need to violate channel usage regulations and dedicated targeting of single vehicles is possible, which is not the case for prior found DOS attacks.

The attacker is assumed as an active advisory using a single communication unit. This means he can receive, store, modify, create and send arbitrary messages at a single point in the network. However, the attacker has no access to valid credentials to sign his messages.

III. General Security Considerations of Data Handling under a VoD scheme

In general, it is recommended to keep the interface exposed to an attacker as small as possible. For example, [13] argues that the format of the security envelope of ETSI ITS should be adjusted to avoid parsing of its content before signature verification takes place. With VoD, the whole message gets parsed on all protocol layers before the decision on whether to verity the message is done [6]. In contrast, verify-all only exposes low level data processing interfaces up to the network layer security entity. Thus, the surface for an attack on data parsing and usage is increased massively by VoD in comparison to a verify-all scheme.

Within ETSI ITS the data sets on various protocol layers use much more complex encoding in comparison to WAVE, for which VoD was proposed. Thereby, protocol layers above the MAC layer use variable length data sets and deeply nested data types [14]–[16]. On the facility layer ASN.1 encoding, e.g., UPER (unaligned packed encoding rules) for CAM and DENM, is used. Parsing of data sets with such complex encoding schemes requires complex implementations leading to many possibilities for security problems. Even for much simpler ASN.1 schemes, like BER (basic encoding rules), many security problems have been found in the past, e.g., the BERserk vulnerability [17]–[20].

Thus, the effort for secure implementation of all functionality handling received data is significantly increased by using VoD in comparison to a verify-all scheme. This puts the VoD concept into question from a system design perspective.

IV. Interaction of Verify-on-Demand and Network Layer Protocols

In the following we separate the discussion of VoD's influence on the network layer into the impact on VANET specific GeoNetworking and IPv6 over GeoNetworking.

A. GeoNetworking

VoD influences greedy forwarding and CBF for multi-hop communication. Such forwarding algorithms need to keep track of locations of nodes in their surrounding [9]. Thus, each received message leads to an update of a neighborhood table. For greedy forwarding members of the neighborhood table are possible forwarders. In case a forwarder gets selected, the message containing the last known position of this node needs to be verified. Otherwise, an attacker could cause forwarding to non existent bogus nodes (neighborhood table poisoning). This would clearly harm further dissemination of the message's content. This affects received messages which should be forwarded as well as multi-hop messages generated by the node itself (e.g., DENMs).

In case of CBF, the neighborhood table is used to determine whether the own node is a possible forwarder of the received message, i.e., forwarding by the own node causes progress towards the destination. This is required as the prior sending node's position is not contained in a multi-hop message [15]. Thus, its position is determined from the neighborhood table using its MAC address. This requires a verification similar to the case of greedy forwarding. Otherwise, an attacker could foil the CBF algorithm by either causing incorrect forwarding or causing failure to forward by the attacked node.

A significant problem of neighborhood table keeping in connection with VoD is the possibility to cause bogus updates, which replace valid entries in the table. Thereby, an attacker uses the ID of a valid node for its own faked messages. In the worst case, a neighborhood table contains no valid entries at all, due to such an attack. To avoid such an attack, mainly three countermeasures can be thought of.

1) One could verify all messages before the neighborhood table update. However, this disables VoD completely, as every message gets verified.
2) Instead of replacing entries in the table, one could keep prior entries, too. Old entries are only removed after a later update got verified. However, this significantly increases memory requirements, due to an expected low number of verifications.
3) One could only store entries in the neighborhood table after the corresponding message got verified. However, low numbers of verifications will cause neighborhood tables to be (very) sparse. Thus, it can be expected that routing will suffer significantly from such an approach.

Thus, usage of a combination of multi-hop communication and VoD is not recommended.

Furthermore, all received messages, which a node wants to forward, have to be verified in advance to forwarding, independent from the used forwarding strategy. This is done to avoid creation of bogus channel load by an attacker [15], [21]. ETSI ITS does not change the signature of a forwarded message. For VoD two main cases have to be distinguished.

1) Verification of a node's position data for forwarding needs to verify a prior received and stored message. Only a central (i.e., cross layer) storage of full messages can avoid multiple verification of the same message by stor-

ing the verification result. However, such an architecture introduces an extra dependency of the network layer and the message storage.

2) Verification of a received and to be forwarded message splits again into two cases depending on relevance of the received message for the receiver.
   a) A receiver outside the message's relevance area only forwards it. Thus, the message is not stored in the LDM, as it never reaches the facility layer. It is only handled by lower layers up to the network layer. Hence, the network layer needs to cause verification by the security entity.
   b) A receiver inside the message's relevance area hands the message over to higher layers and forwards it. Thus, it gets stored in the LDM and the network layer causes its verification, as in case 2a. In case an application finds a message's data to be relevant, it can be used without further delay, as it has already been verified.

Using the LDM as the messages' storage, as suggested in [8], causes a cross layer dependency of network and facility layer as well as interactions of both entities with the security entity. Hence, separation of layers and uniqueness of responsibilities within the protocol stack suffers from such a design.

Instead we recommend a message storage within the cross layer security entity. It can provide a common interface for message verification for all protocol layers.

B. IPv6 over GeoNetworking

IPv6 over GeoNetworking is used to support IPv6 based communication with arbitrary higher level protocols over the dedicated VANET network layer. Such protocols use meta data, whose usage has to be preceded by message verification. However, the core aim of IPv6 over GeoNetworking is to use unchanged standard internet protocols. Thus, the VANET network layer has to ensure verification of all messages passed to an IPv6 interface. Hence, VoD is inappropriate for this kind of communication as every single message has to be verified to avoid attacks on higher level protocols or applications.

V. Interaction of Verify-on-Demand and Certificate Handling

Validation of a message is not limited to checking only its own signature. Moreover, the certificate (chain) used to secure the message needs to be verified, too. Within ETSI ITS there are at most two levels of unverified certificates, which are the pseudonym certificate (PSC) of the sending node and the authorization authority certificate (AAC) which is used to secure the PSC. The AAC is signed using a root certificate known to all nodes in the VANET.

The PSC is individual per node. Thus, a rapidly changing vehicular environment leads to reception of many different PSCs. Hence, a high number of verifications is required for a verify-all approach for PSCs. In contrast, the number of AACs can be expected to be small (see also Section VI). To avoid verification of certificates for messages which are never verified, VoD should be extended to certificates as well. Otherwise, the massive reduction of required verification capabilities as outlined in [6] cannot be reached, due to verification of many certificates.

Unfortunately, even certificates with valid format can become quite large [16], [22]. With a verify-all strategy only validated certificates are stored, but in case of VoD all unverified ones have to be stored, too. Thus, one has to take care that memory for storing PSCs does not become a system bottleneck in case of an attack. Moreover, the verification status has to be stored for each certificate to avoid multiple verifications.

A separate storage for unverified certificates is recommended in case the LDM design from [8] is used. Otherwise, the LDM would also need to keep track of inter-message dependencies of included parts of certificate chains, due to sporadic and on-demand inclusion of certificates [11], [12]. This would add a lot of complexity to the LDM, apart from increasing the interdependency of LDM and security entity.

One should note that this issue does not only affect ETSI ITS, but WAVE as well. For WAVE the situation is even worse, because the corresponding security standard does not limit the amount of hierarchy levels of the PKI system [23].

VI. Efficient Denial of Service Attack

Prior to the actual attack, the attacker stores valid PSCs, which he extracts from received messages. To carry out the attack, a stored PSC is added to the security envelope of a message generated by the attacker. Thereby, the content of the message is chosen in a way to be always regarded as relevant for the attacked vehicle. Relevance criteria can be easily obtained from the definitions of basic safety critical use cases [3]. Moreover, the attacker uses a different PSC, and thereby also different identifiers on all protocol layers, for each message. The messages' signatures consist of random data, as the private keys for the PSCs are unknown to the attacker.

The described attack, enables an attacker to achieve multiple goals at once. These include that for each sent message,

- the receiver regards the message as relevant for itself, which leads to
- message verification including
  1) verification of the formerly unknown PSC, which will succeed and lead to
  2) verification of the signature, which will fail.

Thus, each message sent by the attacker will lead to two computationally expensive verifications. If the attacker can send enough messages to supersede verification capabilities of receivers, he can block or at least delay verification of valid messages. This leads to a successful DOS attack on applications depending on data updates from received messages.

VoD schemes aim to massively limit the requirements for verification capabilities at receivers [6]. Thus, even a quite low number of faked messages, e.g., 10 per second, will exceed the provided capabilities. Thus, the attacker does not need dedicated equipment to jam the wireless channel or increase the channel load by misusing protocol features like described in [11], [12] to perform a DOS attack. Furthermore, the attacker may be able carry out the attack without a need

to violate legal regulations on usage patterns of the wireless channel reserved for VANET communication.

Moreover, the faked messages can be targeted to a dedicated node by using unicast communication at the network layer. Thereby, the attack will go unnoticed by the rest of the network. Both properties reduce the risk of the attacker to be detected and punished.

The attacker can use CAMs and/or DENMs for his attack. Thereby, usage of DENMs enables the attacker to attack all vehicles in the (freely selectable!) relevance area of the DENM. Verification before forwarding (see Section IV) limits the impact to the communication range of the attacker.

The changing identifiers used by the attacker disable simple countermeasures, like blocking of messages from senders after reception of multiple invalid messages. Disabling entire classes of messages, like DENMs containing a dedicated warning type, can only limit the attack if the attacker uses just the blocked dedicated type(s) of messages. However, the attacker could just send a mix of all possible DENMs. Thus, blocking of attacked message types would yield blocking all messages, which leads to a successful DOS attack, too.

The amount of AACs can be assumed to be highly limited. Otherwise, the attacker could send a valid certificate chain (e.g., PSC and AAC) with all elements being unknown to nodes. Thus, three verifications would be required for each message. Within WAVE the length of the certificate chain is not limited. Thus, the number of verifications required to validate a single message can be even higher. However, it can be assumed that the number of higher level certificates will be small in practice. Thus, an attacker cannot provide enough of them to enforce more than two verifications per message.

The described attack resembles the worst case scenario for a VoD scheme, as no verification can be spared. To counter the described attack, a system using VoD would need to have verification capabilities equal to a verify-all scheme. However, this clearly violates the objectives of the VoD design. Thus, the found DOS weakness puts the VoD design into question from a system robustness perspective.

VII. Conclusions and Future Work

Secured communication within VANETs is an important, but yet challenging issue. Reduction of the signature verification load within receivers by verify-on-demand (VoD) schemes is a popular method to limit performance requirements.

The provided analysis shows that VoD leads to a significant number of extra cross layer dependencies. Thus, overall complexity of VANET protocol stacks is increased and separation of dedicated communication layers is reduced. This holds especially for approaches which store to be verified messages within the facility layer LDM, e.g., [8]. Thus, we propose to instead use storage within the cross layer security entity.

Moreover, the amount of interfaces which have to be protected against malformed input from wireless attacks is massively increased by VoD. Finally, the effort for performing a successful DOS attack against dedicated nodes or groups of nodes is significantly reduced by introduction of VoD.

Our findings lead to the conclusion that usage of VoD in the currently proposed form is not recommended for VANETs. Instead approaches of verify-all schemes, like in [5], should be preferred. Moreover, future work could look for more computationally efficient algorithms for securing VANET messages.

References

[1] J. Harding, G. R. Powell, R. F. Yoon et al., "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," Washington, DC: National Highway Traffic Safety Administration, Tech. Rep. DOT HS 812 014, Aug. 2014.

[2] "Memorandum of Understanding for OEMs within the CAR 2 CAR Communication Consortium on Deployment Strategy for cooperative ITS in Europe," June 2011, V 4.0102.

[3] C. Campolo, A. Molinaro, and R. Scopigno, Eds., *Vehicular ad hoc Networks - Standards, Solutions, and Research*. Springer, Dec. 2015.

[4] T. Schütze, "Automotive Security: Cryptography for Car2X Communication," in *Embedded World Conference*, Mar. 2011, pp. 1–16.

[5] M. Knezevic, V. Nikov, and P. Rombouts, "Low-Latency ECDSA Signature Verification - A Road Towards Safer Traffic -," *IACR Cryptology ePrint Archive*, pp. 862 – 877, Oct. 2014.

[6] H. Krishnan and A. Weimerskirch, "Verify-on-Demand - a pracitcal and scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication," *SAE International Journal of Passenger Cars - Mechanical Systems*, vol. 4, no. 1, pp. 536–546, 2011.

[7] A. Weimerskirch, "V2X Security & Privacy: The Current State and Its Future," in *Proceedings 18th ITS World Congress*, Oct. 2011.

[8] E. Koenders, D. Oort, and K. Rozema, "An open Local Dynamic Map," in *Proceedings 10th ITS European Congress*, June 2014.

[9] C. Sommer and F. Dressler, *Vehiclular Networking*. Cambridge University Press, 2015.

[10] H. Füßler, J. Widmer, M. Käsemann, M. Mauve, and H. Hartenstein, "Contention-Based Forwarding for Mobile Ad Hoc Networks," *Elsevier's Ad Hoc Networks*, vol. 1, no. 4, pp. 351–369, Nov. 2003.

[11] S. Bittl, B. Aydinli, and K. Roscher, "Effective Certificate Distribution in ETSI ITS VANETs using Implicit and Explicit Requests," in *8th International Workshop Nets4Cars/Nets4Trains/Nets4Aircraft*, ser. LNCS 9066, M. Kassab et al., Ed., May 2015, pp. 72–83.

[12] S. Bittl and K. Roscher, "Efficient Authorization Authority Certificate Distribution in VANETs," in *2nd International Conference on Information Systems Security and Privacy*, Feb. 2016, pp. 85–96.

[13] N. Nowdehi and T. Olovsson, "Experiences from Implementing the ETSI ITS Secured Message Service," in *IEEE Intelligent Vehicles Symposium*, 2014, pp. 1055–1060.

[14] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, ETSI ES 302 637-2, Rev. V1.3.2, Nov. 2014.

[15] *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-part 1: Media-Independent Functionality*, ETSI ES 302 636-4-1, Rev. V1.2.1, July 2014.

[16] *Intelligent Transport Systems (ITS); Security; Security header and certificate formats*, ETSI TS 103 097, Rev. V1.2.1, June 2015.

[17] E. Whelan, "SNMP and Potential ASN.1 Vulnerabilities," CISSP, Tech. Rep., Dec. 2002.

[18] N. Cottin, "ASN.1 security issues," online: http://powerasn.ncottin.net/download/ASN1_SecurityIssues.pdf, Oct. 2007.

[19] Intel, "BERserk Vulnerability - Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5," Intel Security: Advanced Threat Research, Tech. Rep., Sept. 2014.

[20] ——, "BERserk Vulnerability - Part 2: Certificate Forgery in Mozilla NSS," Intel Security: Advanced Threat Research, Tech. Rep., Oct. 2014.

[21] Buburuzan, T. et al., "Draft C2C-CC Standards System Profile," CAR 2 CAR Communication Consortium, Tech. Rep., Jan. 2014, V1.0.4.

[22] S. Bittl, K. Roscher, and A. A. Gonzalez, "Security Overhead and its Impact in VANETs," in *8th IFIP Wireless Mobile Networking Conference*, Oct. 2015.

[23] *IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, Intelligent Transportation Systems Commitee of the IEEE Vehicular Technology Society Std. P1609.2, Rev. 2013, Apr. 2013.