Secure Broadcast with One-Time Signatures in Controller Area Networks

Bogdan Groza, Department of Automatics and Computer Science, Politehnica University of Timisoara, Timișoara, Romania

Pal-Ștefan Murvay, Department of Automatics and Computer Science, Politehnica University of Timisoara, Timișoara, Romania

ABSTRACT

Broadcast authentication in Controller Area Networks (CAN) is subject to real time constraints that are hard to satisfy by expensive public key primitives. For this purpose the authors study here the use of one-time signatures which can be built on the most computationally efficient one-way functions. The authors use an enhancement of the classical Merkle signature as well as the more recently proposed HORS signature scheme. Notably, these two proposals offer different trade-offs, and they can be efficiently paired with time synchronization to reduce the overhead caused by the re-initialization of the public keys, which would otherwise require expensive authentication trees. The authors do outline clear bounds on the performance of such a solution and provide experimental results on development boards equipped with Freescale S12X, a commonly used automotive grade micro-controller. The authors also benefit from the acceleration offered by the XGATE co-processor available on S12X derivatives which significantly increases the computational performances.

Keywords: Authentication, Broadcast, Controller Area Networks (CAN), One-Time Signatures, S12

MOTIVATION AND RELATED WORK

Intended mostly for the automotive industry, Controller Area Network (CAN) (“ISO 11898-1. Road vehicles - Controller Area Network) is a commonly used bus in cars or general purpose automation applications. All these environments were traditionally isolated in secure perimeters, an image that drastically changed nowadays when control systems (inside a car or not) become potential targets of cyber terrorism. Perfect isolation of a control system environment becomes impossible mostly due to the increased degree of interconnectivity between components and the outside world. A good survey on the subject of security in industrial systems can be found in (Dzung, Naedele, Von Hoff, & Crevatin, 2005) and recent research shows how vulnerable cars are to real-world

DOI: 10.4018/jmcmc.2013070101
adversaries (Koscher et al., 2010). In particular, the importance of assuring security inside a car and on the CAN bus in particular is discussed by Wolf et al. in (Wolf, Weimerskirch, & Paar, 2006).

Here we explore the possibility of using one-time signatures for assuring broadcast authentication at the application layer of CAN. Symmetric key primitives were successfully used in constrained environments such as sensor networks starting with the well known TESLA scheme (Perrig, Canetti, Song, & Tygar, 2001b; Liu & Ning, 2003; Liu & Ning, 2004). But all the TESLA-like solutions rely on time synchronization, an easy to handle procedure but which unfortunately introduces authentication delays that may not be convenient for real-time applications. This happens because the receiver must wait until the disclosure delay expires in order to obtain the key and authenticate the message. Although one can do clever engineering work to improve on this, in many situations it is desirable to have immediate authentication. A version of the TESLA scheme that achieves immediate authentication is in fact available in Perrig, Canetti, Song, and Tygar (2001a) but this scheme addresses the case in which the Message Authentication Code (MAC) of the message is sent before the key disclosure while the message itself afterwards (allowing to authenticate the message when it is received). Here by immediate authentication we want to assure that, as soon as a principal knows the value of the message, he can broadcast it and its authenticity can be checked by receivers as soon as the authentication tag is received.

The only way to achieve immediate authentication is the use of digital signatures. However, digital signatures are more computational intensive than symmetric key primitives, usually of about 3 orders of magnitude, and require more communication bandwidth. The size of a signature varies from several thousand bits with RSA to several hundred bits with ECC. In both cases the computational costs of signing is very high while verification can become somewhat cheap only with RSA. To this, one will need to add the size of the source code as well as memory requirements which are usually limited in industrial controllers. There is still an alternative: the use of one-time signatures which were initially proposed by Merkle in R. Merkle (1979) and R. Merkle (1988). Although they are frequently mentioned in the literature as a cheaper alternative to conventional signatures, they are quite unused in practice, mostly because of their one-time nature. Using Merkle trees makes them viable for multiple uses, but it requires sending an entire path of a tree, and generating, potentially storing this entire tree on the signer side, which leads to even more memory or computational resources. A more general construction, from which the proposals of R. Merkle (1979), R. Merkle (1988) and Lamport (1979) can be derived as particular cases, was provided in (Bleichenbacher & Maurer, 1994) and another work by the same authors studies the optimality of this kind of signatures (Bleichenbacher & Maurer, 1996). A more recent one-time signature scheme was proposed in (Perrig, 2001) and a better alternative to it is provided in (Reyzin & Reyzin, 2002). Thus, there is good literature available on this subject despite a reduced practical impact.

**Contribution**

In a previous short paper we made a brief appointment on the use of an improved Merkle one-time signature for authenticating broadcast in CAN networks (Groza & Murvay, 2011). Here we enhance our previous performance analysis with more details and also implement a more efficient solution based on the HORS signature scheme (Reyzin & Reyzin, 2002). We do find the enhanced Merkle and HORS signatures to offer interesting trade-offs. Indeed, with the HORS signature we exhibit good improvements in the authentication delay since it is more efficient in terms of signature size and verification time. The enhanced Merkle signature also has certain advantages. More, the size of the messages is quite small in most broadcast scenarios since CAN frames carry small data from sensors and actuators (the size of the data field in a CAN frame is actually limited to 64 bits) and the
On Cryptographically Strong Bindings of SAML Assertions to Transport Layer Security
*International Journal of Mobile Computing and Multimedia Communications* (pp. 20-35).
[www.igi-global.com/article/cryptographically-strong-bindings-saml-assertions/58903?camid=4v1a](www.igi-global.com/article/cryptographically-strong-bindings-saml-assertions/58903?camid=4v1a)

Trust Profiling to Enable Adaptive Trust Negotiation in Mobile Devices
[www.igi-global.com/chapter/trust-profiling-to-enable-adaptive-trust-negotiation-in-mobile-devices/169678?camid=4v1a](www.igi-global.com/chapter/trust-profiling-to-enable-adaptive-trust-negotiation-in-mobile-devices/169678?camid=4v1a)