Certificate Revocation List Distribution in Vehicular Communication Systems

Panagiotis (Panos) Papadimitratos, Ghita Mezzour, and Jean-Pierre Hubaux
School of Computer and Communication Sciences
EPFL
Lausanne, Switzerland
{panos.papadimitratos, ghita.mezzour, jean-pierre.hubaux}@epfl.ch

ABSTRACT

The need to evict compromised, faulty, or illegitimate nodes is well understood in prominent projects designing security architectures for Vehicular Communication (VC) systems. The basic approach envisioned to achieve this is via distribution of Certificate Revocation Lists (CRLs). Nonetheless, the problem of how to distribute CRLs effectively and efficiently has not been investigated. In this paper, we addresses exactly this problem. We propose a flexible, simple, and scalable design that leverages on road-side VC infrastructure. Our scheme can distribute large CRLs across wide VC regions within minutes, by utilizing a bandwidth of only a few Kbps at each road-side infrastructure unit.

Categories and Subject Descriptors: C.2.0 [General]: Security and Protection; C.2.1 [Network Architecture and Design]: Wireless Communication

General Terms: Security, Design, Performance.

Keywords: Security, Revocation, VANET.

1. INTRODUCTION

Ongoing efforts to design VC security architectures, e.g., SeVeCom [1], IEEE 1609.2 [2], seek to secure communication and protect private user information. The envisioned VC systems rely on multiple *Certification Authorities* (CAs), with each CA managing identities and credentials for nodes (vehicles and road-side units (RSUs)) registered within its *region* (e.g., national territory, district, county). Each node is uniquely identified and holds one or more private-public key pairs and certificates, digitally signing messages it transmits.

Nodes holding keys and credentials, however, do not necessarily comply with the implemented protocols. They may be faulty or illegitimately obtain private keys [3]. To ensure the robustness of the VC system, it is important to *evict* faulty nodes and prevent the utilization of compromised keys. The distribution of *Certificate Revocation Lists* (CRLs) is the basic approach: each CA adds to its CRL registered nodes' certificates that have not expired yet and it deems it must revoke, and it periodically publicizes the CRL. Providing CRLs across the wireline Internet is a long-known practice that can be helpful in the VC context. For example, in a pseudonymous authentication system, a CRL sent to a provider of short-term VC credentials will expel a node by preventing it from obtaining new credentials [1]. Nonetheless, the distribution of CRLs across the wireless part of the VC system, so that correct nodes can ignore messages signed by revoked nodes, has not been investigated.

In this paper, we are concerned with exactly this fundamental problem: *how to distribute revocation information* across a large-scale and multi-domain VC system, given the constraints and challenges of the VC environment. We design a system, outlined in Sec. 2, able to deliver in a timely manner the appropriate CRL to all vehicles within a region. More important, we show that this can be achieved without densely present road-side infrastructure, without RSU-to-RSU communication, with CRLs that contain only regional revocation information, in the presence of channel and mobility impairments, and without interfering with time-critical VC (e.g., for transportation safety applications). In Sec. 3, we show that with sparsely placed RSUs transmitting CRL data at rates of few Kbps, practically all vehicles can receive securely the complete CRL within minutes.

2. SYSTEM OPERATION

The objective of our system is to ensure that upon issuance of a new CRL, at some time t_0, the CRL is distributed via the RSUs within a delay Δ, to a fraction x of all nodes that circulated in the CA region for at least Δ seconds after t_0. The system design should achieve an x approaching to 1 and a low Δ. Rather than aiming for specific values for Δ, here we investigate the design space to determine which values are achievable at what cost.

We propose a scheme with three basic elements. First, the *collaboration between regional CAs*, so that CRLs contain only regional revocation information and their size is kept low. Second, the use of *encoding* of CRLs into numerous (cryptographically) self-verifiable pieces, to provide resilience to disconnections, radio impairments, and malicious message injection. Moreover, the *low-rate* broadcast transmission of CRL pieces by RSUs, to keep the CRL distribution efficient without interfering with other VC traffic, especially leaving bandwidth available for time-critical VC applications.

The multi-domain CA structure keeps CRL sizes low, but vehicles need revocation information from other regions to validate the certificates of foreigner (visiting) vehicles. Distributing CRLs of other regions in each region would be a costly operation. Instead, we propose that only the CA validates certificates of visiting nodes; if they are not revoked in their home region, it issues them short-lived *Foreigner Certificates* (FCs) which they must use in the foreign region. If

VANET'08, September 15, 2008, San Francisco, California, USA.
ACM 978-1-60558-191-0/08/09.

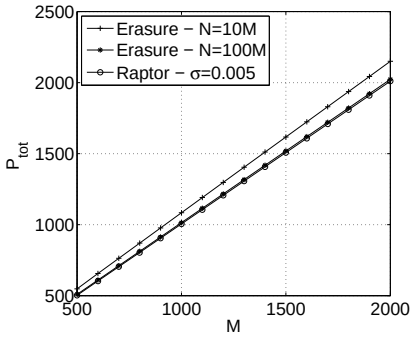

Figure 1: Number of pieces to be received (P_{tot}) vs. number of original CRL pieces (M).

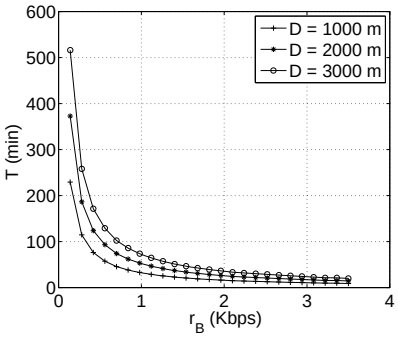

Figure 2: CRL acquisition delay (T) vs. bandwidth (r_B).

the holder of an FC is revoked later on, it is included in the CRL of the CA that issued the FC as an own certificate, and its actual certificate is added to its home CA CRL.

The encoding of the CRL into multiple pieces can be done in different ways, using *Fountain* or *Erasure* codes. Initially, the original CRL is segmented into M parts and then encoded, with added redundancy. Erasure codes produce $N > M$ *CRL pieces*, such that for any M out of N pieces received, the original CRL can be reconstructed [4]. Fountain codes and among them a special class, Raptor codes, with linear time encoding and decoding complexity [5], produce for M input pieces a potentially limitless stream of output CRL pieces. For a tunable parameter $\sigma > 0$, the original M pieces can be recovered with high probability from any subset of $M(1+\sigma)$ CRL pieces. The CRL version and timestamp, a piece sequence number, the CA identifier and a digital signature covering all previous fields, are added to each CRL piece, so that each of them can be validated individually.

3. EVALUATION

We consider the size of the CRL, the average distance, D, between successive RSUs, and the CRL distribution bandwidth, r_B. For more information and findings, due to space limitations, we refer to [6].

Let P be the number of pieces a vehicle receives from each encounter with an RSU, with a fraction of those possibly received during previous RSU encounters. The total number of pieces, P_{tot}, a vehicle needs to receive in order to recover the M segments of the CRL, depends on the encoding scheme. If no encoding but only CRL segmentation is used, $P_{tot} >> M$, resulting in a considerable waste of bandwidth. The benefits of encoding are shown in Fig. 1: Erasure and Fountain codes yield an efficient scheme, with $P_{tot} \approx M$, with the choice of a coding scheme possibly based on its complexity and the existence of patents.

The time, T, over which a vehicle completes the reception of a newly issued CRL with probability 99.99%, captures the effectiveness of the scheme. If s is the size of the CRL data contained in each CRL piece, o is the packet overhead, and v the average vehicle velocity, $P = \frac{r_B}{s+o} * \frac{R}{v}$ is the number of pieces received from one RSU. To complete the reception of a CRL, a vehicle needs to encounter $n = \frac{P_{tot}}{P}$ RSUs. Thus, for a vehicle encountering RSUs separated by distances D_i, $T = \frac{1}{v}\left[\sum_1^{n-1} D_i + R\right]$.

Fig. 2 shows T as a function of r_B for three values of average RSU distance, D, RSU communication range of $R = 300$ meters, original CRL size of 200 KB, and an average vehicle velocity of 40 km/h. D reflects the density of RSUs, which at an early deployment stage will be sparse. T increases with D, as a vehicle needs more time to encounter n RSUs to complete the CRL acquisition. Fig. 2 shows exactly that a moderate increase in r_B quickly brings T down to ten minutes or less.

4. CONCLUSIONS

We present a simple and robust design for CRL distribution in VC systems, leveraging on VC equipment that is to be deployed. We find that with very low bandwidth used for CRL transmissions, practically all vehicles can obtain the latest CRL within tens of minutes, e.g., the duration of a commute. Our analysis reveals trade-offs and how the system can be configured to reduce the CRL acquisition delay. Overall, *scalability* is achieved due to keeping CRL sizes low and due to minimal RSU-CA and no RSU-RSU interactions. As future work, we will investigate how to reduce T further, for given RSU deployments, with vehicles relaying CRL pieces over multiple wireless hops beyond the range of RSUs.

5. REFERENCES

[1] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, and M. Raya. Architecture for secure and private vehicular communications. In *ITST'07*, Sophia Antipolis, France.

[2] IEEE1609.2. IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages, July 2006.

[3] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. Securing vehicular communications - assumptions, requirements, and principles. In *Workshop on Embedded Security in Cars (ESCAR)*, Berlin, Germany.

[4] M.O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. In *J. ACM 36 (2) (1989), 335 – 348.*

[5] Amin Shokrollahi. Raptor codes. *IEEE/ACM Trans. on Networking*, 14(SI):2551–2567, 2006.

[6] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux. Certificate revocation list distribution in vehicular communication systems. In *LCA-REPORT-2008-019.*