A Data Security Protocol for the Trusted Truck® System

S. A. Bulusu, B. Arazi, I. Arel, A. Davis
EECS Department
University of Tennessee
{sbulusu,barazi,itamar}@utk.edu

G. Bitar
Volvo Technology of America
Greensboro, NC
george.bitar@volvo.com

ABSTRACT

Security has become one of the major concerns in the context of Intelligent Transportation Systems (ITS). The Trusted Truck® system provides an efficient wireless communication mechanism for safe exchange of messages between moving vehicles (trucks) and roadside inspection stations. Vehicles and station are equipped with processing units but with different computational capabilities. To render data exchange in Trusted Truck® more secure, this paper proposes a secured data protocol which ensures data integrity, message authentication and non-repudiation. The uniqueness of the protocol is that it effectively exploits the asymmetry of computational resources. It is cost-effective, resource-efficient and is embedded within the Trusted Truck® environment without demanding any additional hardware infrastructure. The protocol balances the computational load between vehicles and stations by incorporating an innovative key transport mechanism. Digital signatures and encryption techniques are utilized for authentication and data confidentiality. Cryptography algorithms along with optimization methods are used for digital signatures. The execution time of the algorithms is analyzed along with clear demonstration of the benefits offered by the proposed scheme.

Categories and Subject Descriptors

D.4.5 [**Security and Protection**]: Cryptographic Controls

General Terms

Algorithms, Performance, Security

Keywords

Trusted Truck® system, secured data protocol, public-key cryptography, key-transport mechanism

1. INTRODUCTION

The US Department of Transportation takes the responsibility to ensure that heavy vehicle carriers are complying with the safety regulations without affecting the time and profitability of these carriers. Intelligent Transportation Systems (ITS) utilize modern technologies and systems in an aim to improve a broad range of transportation systems. The Trusted Truck® project is one such project which allowed the US DOT to significantly shorten carrier verification times by providing a wireless communication link to verify the credentials of vehicles while adhering to ITS standards.

The Trusted Truck® Program was initiated in 2003 as a joint effort by Volvo Group North America, the National Transportation Research Center, Inc., (NTRCI), and The University of Tennessee. The primary vision behind this effort is to provide safe and efficient heavy vehicle transportation. Of particular focus is the ability to present and verifying the credentials of vehicles prior to their approach to inspection offices. Hence, significant time is saved by the truck as well as the inspectors, allowing them to focus more on potential safety violations. The concept behind the Trusted Truck® system is that once a truck is verified, confirmed and labeled as 'trusted' it can bypass other weigh stations. Along with the safe transportation, it is also capable of providing secured communication via a wireless communications link.

2. SECURITY REQUIREMENTS

Information security forms an important aspect of secured wireless communication between vehicles and road side inspection stations. Regardless of who is involved, all parties in any transaction must have confidence that certain information security objectives have been met. For decades, cryptographic techniques have been in employed in order to provide information security and/or secured communication. Modern cryptography can be divided into two classes: symmetric key cryptography and public key cryptography. The former uses the same key for encryption and decryption whereas the latter uses two different keys: one public and the other private. RSA is a public key cryptographic method which has been successfully used for over 20 years in secured message transfers [2][4]. RSA uses a pair of keys for encryption and decryption as well as for digital signatures [5]. Digital signatures are used to verify the authenticity of a particular sender [4]. In most secured communications, RSA is employed for digitally signing and transferring a secret (session) key which is utilized to encrypt messages exchanged by the communicating parties. Upon successful verification of the authenticity of a sender, the secret key is extracted and messages can be encrypted and decrypted.

For the Trusted Truck® system to be secure, a data security infrastructure should be in place such that messages are exchanged only between trusted parties. The necessity for a robust data security infrastructure for such a system initiated the development of a resource-efficient data protocol for the exchange of messages between the vehicles (trucks) and inspection stations. In an environment where critical information is exchanged between the vehicles and the stations, there is always a threat of data manipulation, tampering of vehicle sensors, and inappropriate identification of the participants. This paper presents a cost-effective and resource-efficient secured data protocol which

Conference'04, Month 1–2, 2004, City, State, Country.

has been customized to the Trusted Truck® environment in an effort to provide data confidentiality and message authentication. The paper also introduces an innovative way to use and enhance the speed of an existing asymmetric key cryptographic algorithm to balance the computational load between the vehicle and the road side inspection station. The designed protocol utilizes RSA for the digital signatures and DES [3] for encryption and decryption. The DES key is transported safely through a key-transport mechanism using RSA. Mathematical explanations of the algorithms are provided to support the observed performance improvements.

3. SYSTEM DESCRIPTION

3.1 Communications Framework

The Trusted Truck® system involves three main entities - vehicles (trucks), station (departing station, weigh station, arriving station) and a Certificate Authority (CA). The departing station is the point at which the vehicle's trip begins, the weigh stations are the inspection stations along the highway and the arriving station denotes the final destination of the vehicle. In addition to these there is driver and cargo information which is crucial in the context of vehicle identification at the departing stations. It is important to note that none of the exchanged messages in this model are encrypted. To make this system more secure and protect messages from adversarial interference, a secured protocol is designed which does not modify the structure of the existing system, but rather revises the manner by which messages are exchanged. The protocol is designed such that the identification and authentication mechanisms are embedded in the messages exchanged between the vehicles and stations.

3.2 Secured Communication Mechanism

The designed security protocol utilizes the same link used for communication, with the main difference being that all messages exchanged are strongly encrypted and digitally signed by all participants. The vehicle and the station mutually authenticate each other prior to exchanging messages. Before initiating the communication process, the CA generates and approves all public and private keys for the vehicle as well as stations. The CA is considered an entity which is credible and trusted by all parties wishing to communicate. The CA generates the set of public and private keys for each and every vehicle separately and for the individual stations. The CA's public and private keys are used in the digital signature processes. Once the key generation is complete, every vehicle and each station are loaded with their corresponding public and private keys. The CA also distributes its public key to all vehicles and digitally signs the vehicle/station IDs, expiration date and their public keys using its public key. Expiration date is used for further verification of the vehicle and station, while an ID represents a unique number issued to the vehicle or station. Along with these keys, the vehicle collects and stores, using an onboard unit, all its sensor readings along with cargo details. With all the details ready, the truck initiates the communication process with a station. The nature of the message exchanged depends on the type of station communicated with (i.e. departing, weigh or arriving). The following outlines a series of messages exchanged between the vehicle and the station upon imitation of the communication process:

a) The vehicle receives the station's certificate and, using the preloaded CA's public key, verifies the station's certificate. If all the credentials (ID, expiration date, etc.) are found valid, the vehicle extracts the station's public key from the certificate. This assures the vehicle that it is communicating with the correct station and not an imposture. After obtaining the station's public key, the vehicle uses this public key to encrypt the unique 'Session Key' and send the same key to the station along with its certificate. The Session Key is the key used to encrypt the vehicle details, such as driver ID, cargo information, sensor readings and other related information using the DES algorithm. This key is unique and is generated each time the vehicle communicates with the station. Thus no two stations will receive the same session key. If, on the other hand, the station's details fail to be verified, the vehicle sends a message indicating failure to validate key and logs the result.
b) Upon receiving the vehicle's certificate, the station extracts the ID and expiration date of the vehicle using the CA.s public key. If the received details are found valid, the station proceeds to the next set of messages. The station extracts the session key from the vehicle's certificate using its private key and decrypts the vehicle details using the session key. If any of these details fail to be correctly verified, the vehicle is not granted permission to proceed further and the result is logged.
c) The precise content of the messages depends on the station with which the vehicle is communicating.

This revised secured communication framework delivers all the required services mentioned above, including the verification of the parties' identity at each and every stage and at the same time maintains the confidentiality of the data through encryption. Vehicle details are 8 bytes in length while the cryptographic algorithms operate on data units of length 128 byte or above.

4. KEY TRANSPORT MECHANISM

As mentioned above, in the Trusted Truck® environment, there is an asymmetry between the computational capabilities of the truck and the stations. The truck is equipped with a low-grade, 16-bit processor while the stations are equipped with a PC-level processor system. This greatly varies the time taken by the truck to compute the cryptographic algorithms when compared to the station.

The major operations on the truck side as well as station's side are the signature generations, signature verifications and the encryption and decryption operations. The signature generation using RSA can be done by performing the following operation

$$S = M^{d} \bmod n \qquad (3.1)$$

where M denotes the message, d the private key, n the product of two large prime number p and $q,$ and S is the signed message or encrypted message. The corresponding verification is accomplished by performing

$$M = S^{e} \bmod n \qquad (3.2)$$

where e is the public key or the decryption key. In the designed system, the decryption key is chosen to be e = 3. Lower value of e reduces the number of modular multiplications required and thus decreases the overall time taken to perform (3.2). The private and public keys of the vehicle and the station are 128-byte in length and those of the CA are 144-byte in length. The mathematical operations in (3.1) and (3.2) involve modular exponentiation [1], which is the core time-consuming function. In this system, all cryptographic algorithms operate on 128-byte numbers, so the vehicle with a simple 16-bit processor on board requires more time to compute the core operations when compared to the station which is equipped with a strong processor. Thus the other goal of the protocol would be to balance this asymmetry by intelligently optimizing the algorithms involved. Along with the speed-up in the algorithms, an innovative way of utilizing the travel time has been formulated, namely in the form of an offline key transport method, as described next.

3.1. Offline and Online Key Transport

In this method, the vehicle performs the operations in two modes- offline and online. Here offline refers to the stage where the vehicle is not in the vicinity of an inspection station or the time prior to reaching the next inspection station. The term online refers to the time interval during which the vehicle is communicating with the station and is located in its vicinity. The vehicle uses a method of offline key generation and an online key transportation to send the key to the station.

4.1.1 Offline Key Generation

In offline key Generation, the vehicle completes the generation of the session key and issues a certificate by signing a message (containing the session key and the vehicle ID) using the vehicle's public and private keys. As the session key is used for the encryption and decryption of critical messages, care has to be taken while transporting the session key to the station. Instead of sending the message directly, a message V is framed with the session key in it such that only that specific station is able to recover V and at the same time the station must be assured that a particular and unique vehicle generated message V. If K (8 bytes) is the session key, then the message V (128 bytes) is framed such that

V = {64 bytes of zeros || 4 repetitions of VehicleID ||
4 repetitions of K} (3.3)

This message is digitally signed using the (n_t, d_t) pair,

⍰=⍰⍰⍰⍰⍰⍰ ⍰⍰ (3.4)

where (n_t, d_t) is the public and private key pair of the vehicle and *L* is the digital signature of the message V. The repetitions of the ID and the session key in the original message prevent intruders from modifying the message. The number of repetitions of the ID signifies the known message which is embedded in the original message. Moreover, unlike the standard RSA [6] protocol; here we cannot transmit the original message for signature verification as it contains the secret key (session key). So even the signature is encrypted using the station's public key and later this key is recovered from the extracted message. Let C be the encrypted version of the signed message, then C is given by,

⍰=⍰*3* ⍰⍰⍰ ⍰⍰ (3.5)

where n_s is the station's public key. When the vehicle approaches an inspection station, after authenticating the station, the vehicle sends the session key and it's ID via the online key transport mechanism.

4.1.2 Online key Transportation

In Online key transport the vehicle verifies the station and the vehicle signs the offline generated certificate (containing the session key) using the station's public key. Next, it sends this signed certificate to the station. The certificate is transmitted to the station and upon verification, the station verifies the data sent from the vehicle and issues a decision. As generation of this certificate takes less time when compared to the offline certificate and also requires the station's public key, the vehicle performs this process online.

4.1.3 Session-Key Recovery

In Session Key Recovery the station recovers the session key and decrypts the messages sent by the vehicle by decrypting the signed certificate using the station's public key,

V={Cds mod ns}3 mod nt ⍰⍰< ⍰⍰ (3.6)

The station extracts the session key from the message V. This innovative way of generating the key offline and performing the computations before approaching the station reduces the load on the vehicle as well as saves time for the inspection station.

5. COMPUTATIONAL CHALLENGES AND PROPOSED SOLUTION

In order to overcome the inherent resource imbalance between the vehicles and stations, techniques were used which exploited the asymmetry characteristics. One of the key solutions is the incorporation of the offline key transport method, wherein all the time consuming operations were computed ahead of the communication session. The other important solution is the application of the Chinese Remainder Theorem on the vehicle's side. The modular exponentiation has a higher order of complexity and also consumes more time compared to other calculations. The Chinese Remainder Theorem (CRT) optimizes the time required to perform modular exponentiation, thus speeding up the RSA process. The CRT technique breaks down the exponentiation into parts and then combines them.

By utilizing the CRT, we reduce the time taken for the modular exponentiation by a factor of 4 times. An efficient algorithm for the CRT is described in [6]. We have observed the following:

- *The time taken for modular exponentiation on a 32-bit processor without CRT is approximately 0.25 seconds*
- *The time taken for modular exponentiation on the 16-bit processor without CRT is approximately 0.45 seconds*

This time difference causes a great asymmetry in the communication process whereby the station should be validating a number of vehicles concurrently. In order to balance this inequality, optimizations are made in several ways on the vehicle side. This is done in an attempt to reduce the computational load on the truck, which introduces several constraints at the CA level on the keys generated for the truck. When the CA generates the public and private keys for the truck, it ensures that those keys are always less than the keys generated for the station so that the values calculated on the truck are always less than that at the stations and always take less time.

Let p_t and q_t denote the prime numbers generated for the vehicle and p_s and q_s be the prime numbers for the station. To ensure that the above relational inequality is maintained, the second most significant bits of p_t and q_t are always made zero and that of p_s and q_s are always made 1 (one). As a result, the prime numbers for the vehicle take on the form (10$p_2p_3p_4$......1)$_2$ and the prime numbers for the station take on the form (11$p_2p_3p_4$……1)$_2$. As the numbers are prime in nature, the LSB and MSB will always be 1. All trucks perform offline the session key generation required for the authentication phase. This offline key generation is performed for every communication session before approaching a station, thus saving crucial time. On the other hand, the stations perform all the operations online. The only operation performed by the truck online is the modular exponentiation with the exponent equal to 3, i.e. $A = B^3 \ mod \ N$ where A, B and N are 128 byte numbers. Mathematically, as the operation $A = B^3 \ mod \ N$ simply involves one modulo calculation, it takes far very less time when compared to the operation $A = B^E \ mod \ N$. Thus, when the truck initiates communicating with the station, it does not have to spend much time on computations. The combination of these techniques reduce the computational load on the vehicle and help the vehicle in completing the processing required in a reasonable time frame in the order of hundreds of milliseconds. Upon implementing the CRT on the vehicle, the time taken for the modular exponentiations is greatly reduced.

6. RESULTS

The proposed data security protocol was implemented in ANSI C with no requirement of any additional software components. The computational time is noted at each and every stage in process involved and proper care is taken in selecting the appropriate cryptographic algorithms which will fit the environment. The time taken for the modular exponentiations in both 32 bit and 16 bit is observed and noted. Table 1 details the processing times observed on the stations (32-bit processor) platform in performing modular exponentiation, when implemented both with and without the CRT.

Table 1. Time Estimate for modular exponentiation on a 32-bit processor with and without using CRT

Trial No.	Processing time w/o CRT (secs.)	Processing time with CRT (secs.)
1	0.208438	0.057042
2	0.223449	0.057879
3	0.206945	0.057248
4	0.215324	0.056165
5	0.229685	0.056701
6	0.226190	0.056904
7	0.233663	0.058223
8	0.224079	0.05743
9	0.212913	0.056463
10	0.205311	0.057443
Average	**0.2186**	**0.05715**

However, in this application, the participant that requires speed up is the vehicle which utilizes a simple 16-bit processor. It is found that the average processing time required by the 16-bit processor to compute the equation $S = M^d \ mod \ n$ without using CRT is in the range of 400 to 500 milliseconds. When CRT is employed, the same computation task is achieved in 120 to 130 milliseconds.

7. CONCLUSIONS

In this paper, a successfully deployed novel data security protocol for the Trusted Truck® system is described. The innovative claims involve an offline key transport method which significantly reduces the computational load imposed on the vehicles in real-time. The security services offered include data integrity as well as authentication. The protocol is designed in a way that facilitates embedding of the code in the existing architecture of the Trusted Truck® system without need for any additional hardware or software.

8. ACKNOWLEDGEMENT

This work has been supported by research grant DTRT-06-G-0043-03-U22-06-01 from the NTRCI University Transportation Center or NTRCI-UTC, under a grant from the USDOT Research and Innovative Technology Administration (RITA).

9. REFERENCES

[1] Bruce Schneider "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition 1996.

[2] Introduction to cryptography with coding theory, second edition Wade Trappe, Lawrence C. Washington 2006.

[3] Data Encryption Standard, Federal Information Processing-T. Takagi, "Fast RSA-Type Cryptosystem Modulo pkq", CryptoStandards Publication (FIPS PUB) 46, National Bureau of Standards, 1998, 1462 of LNCS. 1998, pp. 318-326.Washington, DC (1977).

[4] M.O. Rabin .Digital Signatures," Foundations of Secure Communication, New York: Academic Press, 1978, pp.155-168.

[5] R.L. Rivest, A. Shamir, and L.M. Adleman, "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979.

[6] Handbook of Applied Cryptography Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone 1996.

[7] Trusted Truck® Environment, http://www.ntrci.org/