CONFIDENTIALITY ASPECTS WITHIN ROAD USER CHARGING SYSTEMS: THE SWEDISH CASE

Martin Boldt and Bengt Carlsson
Blekinge Institute of Technology, School of Engineering
PO Box 520, 37225 Ronneby, Sweden
Tel: +46 457 385841, Fax: +46 457 27125, {mbo, bca}@bth.se

SUMMARY
In this paper we analyze how a proposed Swedish Road User Charging (RUC) system for differentiated distance based taxation affects the corporate confidentiality of haulers. Each hauler needs to equip all their vehicles with an On-Board Unit (OBU) that continuously send position readings back to a central server, which then is used to calculate the taxation. The fact that the system gather, process, and store information about where the vehicles travel introduce threats to the haulers' corporate confidentiality, e.g. if the position data leak to competitors. We describe threats to various parts of the RUC system, together with protective measures. In the end of the paper we discuss the impact on corporate confidentiality if such a RUC system is introduced, e.g. how would the leakage of position data affect transports conveying sensitive goods such as medical drugs or consumer electronics.

Keywords: Road user charging, road user confidentiality, kilometre taxation.

INTRODUCTION
The European systems for charging heavy goods vehicles are currently undergoing a change to make the users pay more correct external costs that are caused by transportation, i.e., internalisation of external costs. Until now, most systems for charging heavy goods vehicles have been based on a yearly flat fee, which gives the right to use the roads for transport purposes. The current developments are towards systems that charge the users for the distance used, i.e., a distance-based taxation with the potential to discriminate between road type, time of usage, environmental performance of vehicles, etc. Charging for the use of infrastructure is not a new concept. New, however, is the increased ability to reflect the socio-economical marginal costs and thereby contribute to achieving general transport policy objectives and the principles set by the European Commission on fair and efficient pricing.

The Swedish RUC (Road User Charging) system, as proposed in Swedish Governmental Commission [2] is to be distance-based for heavy goods vehicles above 3.5 tonnes and concerns all public roads (but not private ones). In order to reflect the marginal costs principle, the fee should be possible to differentiate with respect to the vehicle (primarily according to different environmental performance classes), time of the road usage, and between different roads. It can be noted that this makes the Swedish RUC system more complex than systems in operation at the moment, e.g. in Germany only motorways are considered. The Swedish system should be harmonized with other European systems existing and under introduction. This implies that system should adhere to the EFC-directive [1] with the purpose of achieving a European Electronic Toll Service for heavy goods, which is interoperable.

In this paper we analyze how the proposed Swedish RUC system impact road users' confidentiality when being geographically monitored. We identify sensitive information

processed in the system and comment on possible threats associated with this information. Where applicable we also present techniques for addressing these threats as a way to protect road user confidentiality. Furthermore we also discuss various opinions among road users regarding the introduction of a nation-wide RUC system based on geographical monitoring.

CORPORATE CONFIDENTIALITY

In this work we analyze how the collected information in a RUC system could negatively affect the confidentiality of haulers as all their transports are monitored as a way to differentiate in relation to tax payment. Since we are set out to study hauler *corporation's confidentiality* within the proposed Swedish RUC system we don't address the concept of *privacy*. Instead we are interested in the problem of securely gathering, use, and store the route information from haulers so that it does not leak to for instance competing corporations.

However, the privacy perspective is also interesting to analyse since Scandinavian hulers already use fleet-management systems meaning that many haulers already are being monitored. However, the information collected in these fleet-management is not used to calculate tax, and it is kept inside the company, or one of the business partners. Another important difference is that within the RUC system case the monitoring is forced upon the haulers by the government, who also take access to the information to calculate the distance-based taxation. All these differences makes the proposed RUC system an interesting subject for a privacy analysis as well.

SYSTEM DESCRIPTION

To shed some light on the design of the Swedish RUC system we include a short introduction to its security design. All haulers have a mandatory device called an On-Board-Unit (OBU) installed into their trucks. As seen in the bottom of Figure 1, the OBU receives geographic positions over GPS, which then continuously are sent to the central servers of the toll service provider. The secure Track Log Recorder is the kernel of the OBU in the Swedish concept. We assume it to be a smart card (IC-card) that stores and generates the Track log from the position and time records that is coming from the positioning and time device. The Secure Track Log Recorder store a batch of records, until reporting criteria is met, attach a sequence number to the batch to enable verification of all information being reported, and finally signs the batch and sequence number to guarantee its validity and to prevent later manipulation. This procedure is selected as a way to guarantee that no manipulation of the data is done at a later time, e.g. this prevent any efforts to generate valid data packages at later moments in the event of a control situation [4].

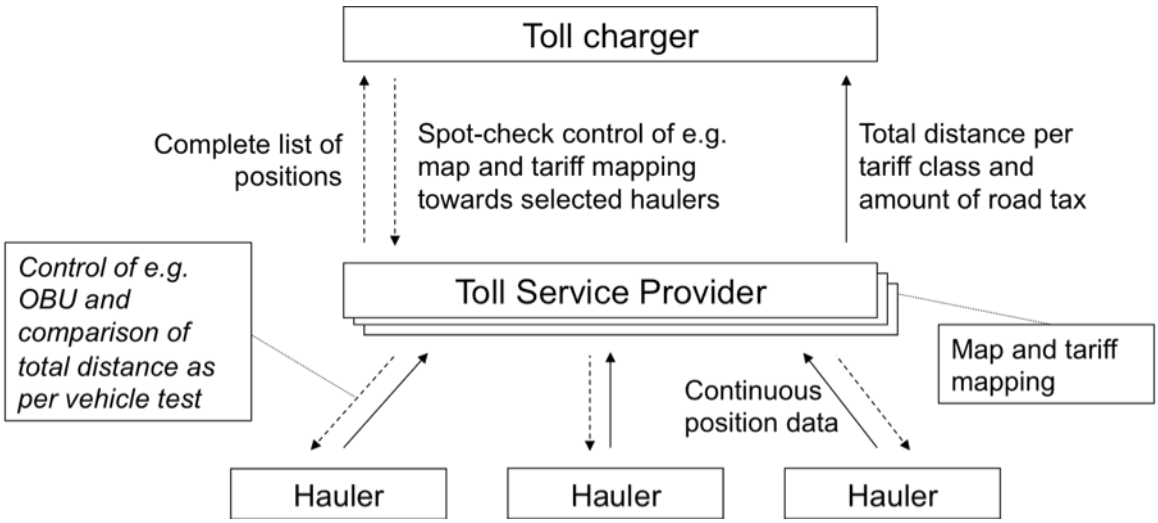

Figure 1. The process of collecting and controlling kilometer taxes.

In Figure 1 a toll service provider is supposed to exist in-between the hauler and the toll charger. The hauler initially establishes a relation with the toll service provider through a contract and thereafter exclusively communicates with the service provider by providing the geographical position data described above. Next, the toll service provider use a map to transform the sequence of isolated positions into a number of road sections that the truck has used, which then is compared to the tariff to calculate the amount of tax. The information specifying the total distance per tariff class is then sent to the toll charger that makes sure that the tax is being paid. At regular intervals spot-check controls are carried out by the toll charger in which the toll service provider is asked to provide the total position data for certain haulers. The toll charger then carry out its own map and tariff mapping to make sure the result is the same as for the toll service provider. Also, during the annual vehicle test the total distance which each vehicle has traveled is compared to the figures sent to the toll service provider.

SECURITY CONCERNS

In a previous analysis we carried out a threat analysis as a way to investigate what security threats that are associated with the proposed system [8]. In this analysis we used the methodology of a standard risk analysis [3] to identify four different assets within the system, i.e. the *OBU*, the *communication infrastructure*, *sensitive data* processed by the system and the *central servers*. Next, threats associated with each of the four assets were identified and mapped into one of the following three different groups; *physical*, *logical*, and *human*. The physical group includes threats that target physical components in the system, e.g. hardware failure or theft. Logical threats target system routines or software, e.g. software failures or denial-of-service attacks. Finally, the group of human threats target threats related to humans, e.g. bribing or social engineering. The order of priority is explained both from the aspect of the hauler and the authority. From a hauler's point of view, a cheating or spying competitor means less business growth. From the authorities point of view there are three threats that must be set aside:

- Large-scale cheating that jeopardize system financing
- Targeted cheating that jeopardize system confidence
- Sabotage that jeopardize system reliability

The result from this threat analysis showed that a number of threats associated with the corporate confidentiality exists. These threats are connected to the asset described as sensitive information, which is described in the next section.

TARGETED INFORMATION

From a confidentiality perspective it is important to analyse what information that is processed by the system, how this information is handled and what negative effects that are connected to leakage of such information. We divide this information in two classes as either *direct information* or *meta-information*.

Direct information consists of the continuous flow of geographical route information, identification data, and time stamps. The combination of these three is found to be sensitive as it could be used to pinpoint a certain road user to a specific road segment at a particular time. However, the information that is sent from the toll service provider to the toll charger in the normal case is not sensitive, since this only include the total amount per tariff class that should be paid, i.e. no geographical positions could be revealed.

Meta-information describes the different types of patterns that appear when analysing the information described above. When aggregating such information it is possible to get a detailed view of the routes that road users have travelled on during vast period of times. This information could reveal what customers a certain hauler has. It could also be possible to calculate how efficient haulers are when it comes to keeping their vehicles running. Different views on whether this information really is confidential or not is presented in the discussion section.

CONFIDENTIALITY THREATS

The confidentiality threats connected to both the direct and meta-information in the system could be divided between three different system parts; the *on-board unit* (OBU), *the communication infrastructure*, and the *central server*. Threats against the OBU are mostly focussed on tampering and various kinds of physical manipulation to attack its integrity. By manipulating the OBU it could be possible to covertly forward sensitive information to third parties, i.e. allowing them to monitor the attacked hauler without his knowledge. Although it is quite easy to protect against these threats, if originating from a novice or medium skilled attacker, it is much harder (if at all possible) to fully protect against highly skilled and equipped attackers.

Threats associated with the communication infrastructure are concern confidentiality and integrity of the information in transit. Eavesdropping on the data communication could allow third parties to gather route information from road users. However, if third parties could intercept the communication they could also carry out an active attack with the aim to modify the data, an attack of the data integrity. Similar threats are found in cellular networks and any other radio-based communication form and because of this there are several off-the-shelf solutions available relying on different types of cryptographic techniques, which we come back to in the next section.

All collected information is gathered in the central server, which therefore is an interesting part of the system for a potential attacker. Since the collected information is the foundation for a calculating road user taxes it must be stored for a period of 10 years according to Swedish legislation. As a consequence a lot of information will be gathered, which could reveal detailed patterns about, e.g. what routes certain haulers use and at what times. Failing

or mis-configured access control mechanisms on the central servers represent one threat towards road user data. Various threats focusing on human administrators are also represented here, e.g. where database managers are bribed to copy data from this central repository. Bribing employees to hand out sensitive information is a well known risk which has manifested itself numerous times in the past, e.g. when employees at telephone companies sell lists of calls on the internet. The threat from social engineering is also present as such techniques could be used to persuade human administrators at the central server to deviate from the security routines and hand out sensitive information, i.e. they are fooled to hand out sensitive information to solve some intricate problem. Still other threats include accidental leakage of data, e.g. during backup management. For some of these threats there exist efficient protection techniques, but others are harder to address as explained in the next section.

PROTECTION TECHNIQUES

In the previous section we discussed security threats affecting confidentiality within the proposed RUC system. These threats could be divided between the OBU, communication infrastructure and the central servers. As a consequence a set of protection techniques need to be considered when constructing the proposed RUC system if the corporate confidentiality should be protected.

OBU Tamper Protection

Since the OBUs are installed into the haulers vehicles they have the possibility to physically tamper with the device to gain some benefit, e.g. to pay less tax. From a confidentiality perspective it is important to secure the OBU so that it can be used as a foundation when setting up protection mechanisms to protect sensitive information, e.g. to store cryptographic keys. Therefore the OBU needs to be protected against modification so that it could be trusted to deliver the services expected from it. The use of smart cards provide such tamper resistance at the same time that it is based on standard technology that could be bought off the shelf [7]. To be able to modify the secure kernel for the OBU on the smart card the attackers need to have firm knowledge in both computer hardware and software, which push the odds in favour for the RUC system providers. However, it is important to understand that it is impossible to develop a fully tamper resistant device if the customers have physical access to them, as the haulers have to the OBUs.

Even though it is impossible to develop a 100 per cent tamper-proof OBU it is possible to raise the bar for a potential attacker. Various obfuscation techniques could be used in this word. The idea is to make it as hard as possible for attackers that have physical access to a device to understand its design. Understanding the design through analysis is a prerequisite to break any security scheme. Of course breaking the security schemes are needed before the device could be modified after the attackers own choice. Two interesting obfuscation techniques involve *runtime encryption* and *integrity verification* [6].

Runtime encryption is based on that all the software except for a small portion in the beginning is encrypted when stored on the smart card. Only when the program is executed is the software decrypted by the small non-encrypted part and a cryptographic key. As a consequence, the decrypted software is only available in clear text under the short amount of time of its execution. Furthermore, the clear text version of the software is only available in the memory of the OBU, i.e. not in its long time storage on the smart card. This will have the effect that a potential attacker must analyse the OBU software as it executes inside the OBU device which is must harder than only analysing the smart card. However, it is important to

understand that a highly skilled attacker could identify the cryptographic key stored on the card and use this to decrypt the software. As we pointed out before, there exists no 100 per cent tamper-proof technique. But the attacker might think the price is too high trying to break the security of the OBU and therefore give up in favour for easier targets. Integrity validation involves including sanity checks within the software itself in key positions of the software. That way it is possible to detect if the software or the OBU is being tampered with, e.g. locking the system down if any data has changed in an unfamiliar way. Combining runtime software encryption with integrity verification could together with the tamper resistance of smart cards provide an interesting solution against OBU modifications. On the negative side is that all these tricks increase complexity and the risk of faults.

Protecting the Communication Infrastructure

Since the proposed Swedish RUC system use GPS/GPRS to transmit the position data from the hauler's OBUs to the central servers it is important to protect this data in transit. However, the threats to the data are identical to ordinary voice or data communication in cellular networks, which also means that standard protection techniques are available. In this case additional end to end encryption could be used between the OBU and the central servers using some of the standardized synchronous or asynchronous encryption schemes [5]. The secret keys could be stored on the smart card, which also solves the otherwise often troublesome task to distribute encryption keys in a secure way. Using such a setup would protect the communication data from eavesdropping.

Protecting the Central Servers

All position data gathered from all haulers end up on one of the toll service providers' central servers. The data needs to be stored for 10 years according to Swedish legislation since it is the basis for tax calculation. If there are any complaints about how the tax has been calculated in some special case the data must be available for later verification. Storing the data for this long introduces problems according to corporate confidentiality since the haulers' detailed positions for several years are stored in digital format. If this data leaks in one way or other it gives a detailed picture of exactly what routes each vehicle in the haulers' fleet has used in the accuracy of meters. The route information of course include the start and end positions that could be used to pin point what company that was the transportation customer. To avoid this it is important to protect the data stored on the central servers and carefully think about how the data is used.

The data stored on the servers should be adequately encrypted and the keys should be strictly handled. This would provide some protection if the data for some reason leaks to a third non authorized party. However, the data needs to be available since it is used to for instance verify tax calculations or to allow the toll charger to check that their toll service providers perform map and tariff mappings correctly. In addition to this the system administrators need to be able to test and maintain the system, which often implies extended privileges. Therefore threats associated with the personnel using the system emerge. Such threats include scenarios based on accidents, e.g. where personnel makes a mistake that result in that sensitive data leaks, to personnel that are being bribed to leak sensitive information exchange to money. To address such threats measures should be taken that keep track of exactly what information each personnel has access to. This way it is possible to trace back-wards exactly who had access to certain data in case of data leakage. Similar techniques are being used in medical care systems. It is also very important to determine exactly when human actors have access to the data in the system and mark special attention to these places.

Another threat to the haulers corporate confidentiality comes from the use of anonymized data for research or statistical purposes. The problem is that it is next to impossible to withdraw useable statistical data from databases without interfering with privacy, or in this case corporate confidentiality. In the next section we discuss a number of interesting points within RUC systems and corporate confidentiality.

DISCUSSION

After interviewing Swedish haulers it is not all that clear whether or not the route information collected in the RUC system should be considered sensitive. This is a matter where opinions divide. On one hand it could be argued that the information written on the containers and lorries (branding) could be used to deduce what hauler that is travelling where, e.g. by standing next to the road and observe what haulers that pass by. It was also pointed out that this could be done at the gates to key customers, which would render in a pretty detailed picture of which hauler that is associated to a certain customer. However, it is quite obvious that this scenario could not be compared to the introduction of a RUC system, that systematically and continuously monitor of road users, resulting in a holistic view of all transports and routes. This holistic view could not be compared to spotting traffic on the roadside.

Another argument for that the route information should be protected include sensitive transports (e.g. medical drugs or consumer electronics such as cellular phones). Such transports are subject to criminal activity and it is therefore important that the route information is protected since the knowledge of previous routes could be used to deduce future ones. It is therefore a plausible that more transports face the risk of criminal activity if the route information is being available outside a trusted community. This is something that probably would be highly disliked by the drivers of such transports, which potentially could develop into a workplace safety issue.

Finally, we believe that RUC system is interesting for questionable actors even if the information processed by the system could not be obtained. The reason for this assumption is that illegitimate road users with antagonistic intentions will try to escape (or at least minimize) the amount of distance-based taxation being charged. Since the amount of such taxation is high these activities could provide an incentive for commercially driven (and questionable) actors to develop methods and technology to circumvent the RUC system in a systematic fashion. The whole concept could be implemented into a product, which is sold under the guarantee that it minimizes the charged tax. It is especially serious since the potential attackers that engage in such a project are business-driven meaning that they have probably both resources and knowledge. Against such attackers it is next to impossible to develop a secure OBU if the attackers gain physical access to the device. In the end this turns out to also introduce implications on road user confidentiality since the security of the OBU has been compromised.

CONCLUSION

In this paper we analyse how a proposed RUC system for calculating distance-based tax calculation for all roads in Sweden affect the corporate confidentiality of haulers. A set of security threats with regard to corporate confidentiality is identified and it is determined that the integrity of the OBU needs to be protected against tampering. Furthermore it is important to protect the data as it was sent to the central servers using normal cellular networks. However, the most important problem to solve is to store all gathered position data on the central servers and at the same time allow the data to be used within the system.

ACKNOWLEDGEMENTS

This work is funded by the Arena project (http://www.arena-ruc.com/).

REFERENCES

1. "Directive 2004/52/CE ", http://ec.europa.eu/dgs/energy_transport/tenders/doc/2006/s44_045846_certification_en.pdf (2008-02-18)
2. "Skatt på väg (SOU 2004:63)", http://www.regeringen.se/sb/d/361/a/24111 (2008-02-18)
3. Thomas R. Peltier, "Information Security Risk Analysis", CRC Press LLC, Boca Ranton, USA, 2005
4. Ulrik Janusson, Thomas Sjöström and Jonas Sundberg, "A kilometre tax for heavy goods vehicles in Sweden – A conceptual systems design", 2007
5. Bruce Schenier, "Applied Cryptography", John Wiley & Sons, Minneapolis, USA, 1996
6. John Viega and Gary McGraw, "Building Secure Software", Addison-Wesley, Indianapolis, USA, 2002
7. Ross Anderson, "Security Engineering", John Wiley & Sons, Minneapolis, USA, 2001
8. Bengt Carlsson and Martin Boldt, "Security Analysis of the Swedish Road User Charging System", submitted to the 15th World Congress on ITS