Using Searchable Encryption to Protect Privacy in Connected Cars

Matthias Matousek, Christoph Bösch and Frank Kargl
Institute of Distributed Systems
Ulm University
{matthias.matousek, christoph.boesch, frank.kargl}@uni-ulm.de

***Abstract*—Providing vehicles with extended connectivity introduces new opportunities for services, and also security applications such as misbehavior detection. However, for many applications, personal data needs to be processed by the system providers, which impairs the privacy of the vehicle users. While focusing our research on new possibilities of connected car security, we follow *privacy by design* principles. We explore the utilisation of various privacy-enhancing technologies (PET) in order to provide advanced connected car applications, while preserving the personal data of the vehicle users. Specifically, we aim to develop practical schemes that utilise Searchable Encryption to provide a framework for secure and privacy-preserving connected car applications.**

I. Introduction

Connected cars are a growing topic for car manufacturers. Most automotive brands now offer services that provide control or information querying of vehicles via web interface or smart phone app. As soon as a specific vehicle is paired with a user account, the owner can use services such as the localisation of his car, querying information like travelled distance or gas usage, and even remote control some functions such as heating or unlocking and locking doors.

As the trend of connected cars leads to more and more data about vehicles being saved and processed in back end systems, the security of theses systems needs to be considered. Additional connectivity and services may increase the attack surface of modern vehicles, but it also increases the potential for detection and prevention of misbehavior and malfunction. Thus, our research focuses on new methods to utilize connected car data in order to perform misbehavior detection and security event management on a fleet-bases.

While security monitoring systems for connected cars are a promising approach, it also raises the question of user privacy. For such a security system, large amounts of personal data need to be processed. A personal vehicle often accompanies its users wherever these travel, thereby collecting large amounts of information on their whereabouts, behaviour, and possibly even lifestyle.

Research has shown that having access to specific car data allows adversaries to deduce further information, such as identifying behaviour or the identity of the corresponding individuals.

Thus, the privacy of car users requires protection. The users' trust in a provider or vendor should not be violated. Further, even when the manufacturer shows only good intentions, data should also be secure when it is leaked due to circumstances such as hacking attacks on the provider back end. Moreover, legal subpoenas that require businesses to hand over their users' data, as well as other attempts to access private data such as surveillance programs, unsettle customers. The usage of a vehicle often accurately reflects its owners' behavior, and thus the generated data needs to be protected.

II. User Privacy through Searchable Encryption

Searchable Encryption (SE) [1] is a promising technology in an approach to provide fine-grained access control for encrypted data. The idea of SE is to enable search algorithms to work on ciphertexts without the need of prior decryption, and without even the need to have knowledge of the corresponding secret key.

A. Searchable Encryption

Generally, two approaches for SE schemes exist. One approach is to use a specialised encryption scheme that allows the ciphertext to be searched directly (e.g. Song et al. [2]). Index-based schemes, however, have better search performance and allow for arbitrary encryption ciphers. Thus, we focus on the latter approach.

While the client (the entity that generates and encrypts the data) is always able to access his data, he can also generate a so-called trapdoor to enable another party to perform a search on the encrypted index. The trapdoor is bound to the specific keyword that it was created for. Thus, the client can limit access to particular data.

In general, a SE scheme consists of the following four algorithms:

- $K_C(\lambda)$: This algorithm is run by the client C, takes a security parameter λ as input, and outputs a secret key K_C.
- $I(K_C, D)$: This algorithm is run by the client C, takes a key K_C and data items D as input, and outputs an encrypted index I, which allows to search D for specific keywords (using a trapdoor).
- $T_s(K_C, s)$: This algorithm is run by the client C, takes a key K_C and a search keyword s as input, and outputs a trapdoor T_s.
- $X(T_s, I)$: This algorithm takes a trapdoor T_s for search keyword s and an encrypted index I as input, and outputs

the query result X. This might be a handle to the (encrypted) data entry or the data item itself

In the vehicular context, data that is generated and collected within a vehicle should be sent to and stored on e.g. a back end server or shared with third-party providers. In order to protect it from unauthorized access, all data is encrypted before it leaves the car. Using SE, the user may generate trapdoors that allows the back end provider to access specific data, and thus to process it without breaching the users' privacy. Similarly, SE can be utilised to manage access for several parties, thereby allowing third-party services.

Depending on the use case scenario, the server requires more or less access to data. In some cases it might suffice to learn whether a given keyword is present in the ciphertext. Often, however, additional knowledge is required. Different SE schemes can provide further access. Schemes that allow for range queries can be used for data that is within certain limits [3], and decryptable SE can even give the trapdoor-holder the ability to access the plaintext of the search result [4].

B. Application Scenarios

Many applications could benefit from the privacy protection that can be achieved with SE, while at the same time being able to function normally.

Pay-as-you-drive insurance policies (PAYD) are a recent trend that bases the costs of an insurance policy on driving behavior. It has the potential to be a fairer alternative to traditional blanket coverage, but introduces severe privacy issues. SE could be used to ensure that only necessary data is accessed. E.g. range queries could be employed to determine whether acceleration regularly exceeds a certain threshold, or the vehicle is driven at night time.

Connected car services and the security of connected vehicles are our primary interest for the application of SE. Similarly to the PAYD scenario, other services could be limited to their required data with SE schemes. We are specifically interested in determining whether SE can be used to enable a back-end-located misbehavior detection that is privacy-preserving.

C. Discussion

For applications within connected vehicles other cryptographic primitives could be thought of, that might be applicable to the presented use cases. This raises the question whether SE is better suited.

Secure multi-party computation has the goal to let several parties compute functions, while keeping their respective input data private [5]. While this is fitting for the envisioned use cases, it would require frequent collaboration of the vehicle with the back end servers. This is impractical for vehicles in deployment. The back end needs to handle potentially large amounts of data quickly. It thus cannot rely on communication with all the vehicles, which might not even be reachable all the time.

Functional Encryption (FE) is a related technique that can be used to perform computations on encrypted data and gain access to the computed result in cleartext without requiring the secret key to the ciphertext [6]. However, most implementations of FE only achieve low performance. SE is currently superior in this regard.

While SE is relatively efficient in regard to computing complexity, it has several limitations. It remains to be evaluated whether it applies to all of our use cases, and whether it is flexible enough to be used in the automotive context that constantly progresses and introduces new applications.

III. Conclusion and Future Work

We proposed the application of Searchable Encryption (SE) in order to provide fine-grained access control to vehicular data of connected cars. Due to its good performance, it is suited to provide privacy protection even in scenarios where large amounts of data are processed. In addition to merely identifying present keywords in a ciphertext, SE can also provide further access to the encrypted data—such as ranges of numeric values, or even the cleartext of search results.

Future work will consist of the identification of the required data processing capabilities, and whether SE can be applied to the given scenarios. We are specifically interested in performing misbehavior detection over an entire fleet in the back end.

In addition to the assessment of suitable schemes, we are planning to implement a novel protocol for privacy-preserving data sharing using SE in the automotive context. A subsequent evaluation of the system is expected to provide us with insights on its usability, applicability and performance.

The eventual goal is to provide a framework that allows for data sharing with strong privacy protection for different applications.

References

[1] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A survey of provably secure searchable encryption," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 18:1–18:51, Aug. 2014.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp. 44–55.

[3] D. Boneh and B. Waters, *Theory of Cryptography: 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, ch. Conjunctive, Subset, and Range Queries on Encrypted Data, pp. 535–554.

[4] T. Fuhr and P. Paillier, *Provable Security: First International Conference, ProvSec 2007, Wollongong, Australia, November 1-2, 2007. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, ch. Decryptable Searchable Encryption, pp. 228–236.

[5] O. Goldreich, "Secure multi-party computation," *Manuscript. Preliminary version*, pp. 86–97, 1998.

[6] D. Boneh, A. Sahai, and B. Waters, *Theory of Cryptography: 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, ch. Functional Encryption: Definitions and Challenges, pp. 253–273.