Yes, Governments Can! - Concept and Experiences with Guaranteed Blindness in a Central Exchange Service

Michael Schafferer[1] and Thomas Grechenig[1]
[1]Industrial Software (INSO), Vienna University of Technology, Vienna Austria
(michael.schafferer||thomas.grechenig)@inso.tuwien.ac.at

***Abstract*- With April 1st, 2012 the implementation of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services, or of public communications networks came into effect in Austria. With this implementation, not only the obligations of the providers of telecommunications services are controlled with respect to the retention of communications data, but also the powers of the security and law enforcement authorities with respect to request both retention data as well as traditional connection data (e.g., security police in the course of fulfilment of affairs). To make the retrieval of such data as transparent as possible, legally secure and traceable, all requests (with only few exceptions) must be carried out only via the so-called DLS, a central exchange service. This allows preventing unauthorized or hidden inquiries practically and not just legally. Both requests and replies must be transmitted only over HTTPS connections to the DLS and must further be secured using end-2-end encryption, enforcing a blind central service.**

Downloaded from www.edlib.asdf.res.in

I. Introduction

In her book on publicity rights, Gillian Black proposes that privacy is the desire of an individual to be free of intrusion [1]. The European Convention on Human Rights states, "that everyone has the right to respect for his private and family life, his home and his correspondence"[1]. This right may be restricted to a person of public interest or for the purpose of prosecution, though this might have to be seen very controversial [2].

Austria was faced exactly with this problem over the course of the implementation of the European Data Retention Directive. Here two controversial subjects have to be dealt with at the same time. First, the infringements of the right of every Austrian citizen for his privacy by the data collection itself, as well as a safe handling during processing and especially transfer of such data between authorities and providers. The aim pursued was accordingly to install a system that conforms to the requirements of the directive and to protect the privacy of Austrian citizens.

The approach the authors designed and partly implemented for Austria, deliberately does not use the handover interface defined by ETSI[2] and tries to prevent the concerns that largely rely on the judgment of the German Federal Constitutional Court [3], as well as various other considerations [4][5][6].

II. State of the Art for Privacy in Governments IT-Infrastructures

Vrakas *et al.* [7] states, "that it has been proved that privacy concerns are a main antecedent of trust in e-government systems intention of use. Therefore, information systems that are not privacy aware are not trusted and thus not accepted by citizens". They argue that conventional ways for preventing attacks on the data's' privacy by mainly employing Privacy Enhancing Technologies (PETs) must involve an organizational context for selecting the appropriate technical, organizational and procedural countermeasures for building privacy aware systems.

[1] http://human-rights-convention.org/
[2] http://www.etsi.org/

DOI: 10.978.819252/12219

A short overview of privacy in the context of digital government is given by Vaidya [8], by examining potential concerns and causes of privacy breaches. This work was based on existing laws regarding privacy, as well as some of the technological solutions and potential challenges. It therefore stresses the importance and responsibility of preventing data misuse coming along with the increase in data being collected, stored, and analyzed.

Haryadi and Malik [9] give recommendations for governments on how to setup a Data Retention System in his paper. It describes points of recommendation to National Telecommunication Regulatory Bodies in establishing data retention regulations and deals with fundamental questions, as e.g., functionalities, logging and site of storage. Moreover, it takes into account the matter of data exchange by taking the example of the European Telecom Standards Institute (ETSI) handover interface.

III. GOVERNMENTAL DATA RETENTION

Government triggered data retention in common has the objective of surveillance, as they, especially their law enforcement, realized the importance of communication data concerning the fight against crime and terrorism. Therefore, a growing number of countries enacted legal backgrounds for the interception of communication data in case of serious suspicions. In addition, e.g., the European Union (EU) enforced "The Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks (2006/24/EC)", known as the Data Retention Directive (DRD) [10]. According to this Directive, every EU member state must retain specific communication parameters of their users for the period of six months up to two years for the purpose of the investigation, detection and prosecution of serious crime. This paper will later on refer especially to this directive.

A. Data Retention Principles of the European Data Retention Directive

In their paper, Haryadi and Malik [9] present recommendations to establish data retention regulations for countries. When it comes to technical aspects they state that the most advanced technical guidelines in Lawful Interception (LI) Data Retention is the collection of ETSI technical specifications and technical reports[3]. Presumably most of the member states implemented the DRD according to these specifications.

One of the standards, the ETSI TS 102 657, deals with the aspect on how to handover retention data from a provider to an authority. It gives a reference model showing a principle setup. This reference model is depicted in Fig. 1. An entitled authority requests data from a communications provider using a defined handover interface. As the figure shows, the Receiving Authority in some cases might not be the same as the Issuing Authority. The Issuing Authority sets the request to an Administrative function in the provider's data retention system. According to the request the provider fetches the data from its database using the Data Store Management Function and transmits it to the defined Receiving Authority. The provider internally feeds his Data Storage from different sources, as e.g., email, Internet access, Internet telephony, mobile telephony, fixed network telephony and so on, using a Data Collection Function. The standard also defines a Log Functionality for event logging of the activities in the Data Retention system.

[3] http://www.etsi.org/standards

DOI: 10.978.819252/12219

Downloaded from www.edlib.asdf.res.in

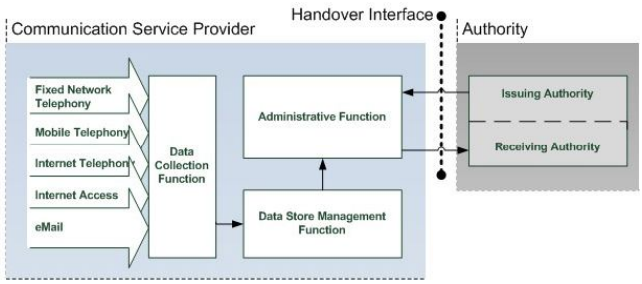

Figure 1. Data Retention System Reference Model

B. Regulations by the Directive to Guarantee Retained Data's Privacy and Security

Concerning processed retention data's privacy and security the directive enacts several regulations to guarantee their confidentiality, integrity, unlawful access and alteration as well as accidental loss. Moreover, it clarifies that the regulations of the Data Privacy Directive (DPD, 95/46/EC) and of the Directive on Privacy and Electronic Communications (DPEC, 2002/58/EC) are furthermore applicable as far as no specific regulations are stated. Basically, from a data security point of view, retention data are to be treated and protected equally to operational data processed in the provider's system providing the corresponding communication service, as far as specific regulations do not require the implementation of stricter measurements. So pursuant to this the provider has to implement organizational and technical measurements and procedures that only authorized staff are able to access retention data and that retention data are deleted after their compulsory period of storage. Moreover, each Member State is engaged to designate one or more national supervisory authorities, which is responsible for monitoring and ensuring an appropriate level of data security [10].

C. Reservations Concerning the ETSI Handover Interface

As part of the implementation of the DRD in Austria some concerns about the ETSI standard for a handover interface have been raised. Due to data protection reasons, access via a direct interface to the database systems of providers was a controversial subject, since it may potentiate the infringement of European privacy law. The concept of the ETSI interface allows a so-called grid investigation within all covered communications data of the DRD. This circumstance corresponds to a kind of data mining. The associated possibilities of linking data goes far beyond the competence of the DRD and therefore was seen as a not acceptable method [11].

In addition, the evolutionary history of the ETSI standards and the contribution of experts from different intelligence organizations give enough reasons for certain suspicion concerning the underlying background intentions[4].

IV. The Austrian DLS - A Central Exchange Service for Retention Data

For the data exchange the directive states that, "Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law" [12]. By following this and due to the aspects mentioned in chapter III-C, we developed a construct not following the ETSI standards for Austria. Amendments in the Austrian Telecommunications Act regulate exactly which data may be requested by authorities under what conditions. An

[4] https://moechel.com/lectures/

DOI: 10.978.819252/12219

Downloaded from www.edlib.asdf.res.in

associated technical Data Security Decree gives a holistic legal as well as technical solution for the mandatory system to exchange this data between authorities and provider, on the basis of official request letters (in PDF format) and defined response files (in CSV format) [13]. The fundamental challenge was to develop this system with appropriate level of privacy while allowing secure communication and data transfer between providers and entitled authorities. In addition, the superior requirements of the DRD had to be met.

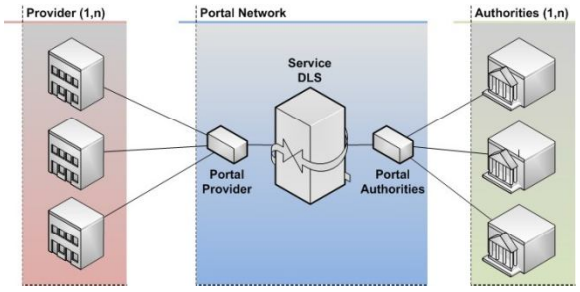

Figure 2. The Principle Concept of the Central Exchange System (DLS)

For this, we introduced an oriented hub-and-spoke architecture with a central trusted third party (the so called DLS), allowing data transmission only between provider and authorities. The basic construct is shown in Fig. 2. The framework builds on a central exchange service, embedded as a service in the so-called Federal Portal Network (short PV). Access to this service is made possible only by one portal each for providers and authorities. This setup enables a transparent, legally as well as technical, secure data exchange service with the possibility to trace every event for requesting data.

A. Guaranteed Blindness of the Central Exchange Service

As already mentioned, the DLS represents a kind of hub for information on communication and retention data. To ensure data security and privacy, data should only be exchanged in a confidential way. Therefore, the DLS is designed in a way that the content transmitted in requests and responses cannot be inspected by the DLS, even with the content not being accessible to system administrators. The system as a whole can only be compromised if a client itself is compromised and per design should not provide possibilities to intercept information, neither by active MitM attacks, nor by passive eavesdropper. This requires strong cryptographic measures with encryption of both, the request and the response, already in the infrastructure of each actor, and consequently before being sent to the DLS. Additionally, the data transmission between clients must be secured at the transport level.

The transmission is secured with a transport encryption based on HTTP Secure (HTTPS), using proven technologies enforcing HTTPS/TLS[5] 1.2. As stated in the corresponding RFC 5246, "the protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery."

Additionally to the transport encryption, the actual content of a request and the corresponding answers must be encrypted as well. For this, a hybrid encryption method based on a Public Key Infrastructure with symmetric session keys is used. Therefore, it is achieved that the data can be decrypted only by the dedicated receiver. This also ensures the appropriation of the data to its objectives according to the Directive. Thus, the demand of the blindness of the DLS for the exchanged data is fulfilled.

[5] http://tools.ietf.org/html/rfc5246

DOI: 10.978.819252/12219

Downloaded from www.edlib.asdf.res.in

The public and private key are specified to use RSA-2048 bits for client certificates, and RSA-4096 bits for the Root certificate, while the used symmetric session key has to follow the specifications of AES-256 in CBC mode, using PKCS5 padding (also known as Standard Block Padding). This is conforming to the recommendations of the BSI[6] for secure key material [14].

B. The Rollout-Concept of the DLS

The DLS presents its users specialized clients in form of a web application, depending if they are an authority or provider. The clients are implemented based on *HTML* and *Java Script* in order to run entirely in a web browser, while including all designated use-cases and functionalities stipulated to authenticate, set and get requests, encrypt and decrypt data, digital sign data and check digital signatures, as well as to provide required statistics. These clients satisfy all legislative as well as technical requirements of the Data Security Decree (DSID). These clients must authenticate using the corresponding Access Portal to logon on to the DLS.

The unusual approach to perform all cryptography in the browser instead of using external software also revealed the need to generate the symmetric AES key inside the browser. At the time of implementation, there was no possibility to utilize a key generator or random number generator provided by the operating system. Therefore, a concept for the creation of the required symmetric session keys inside the browser was required. In order to accomplish this for the web application provided by the DLS, different sources for filling entropy pools had to be used. The mentioned sources gather information which are collected in entropy pools, which will be utilized by the Fortuna pseudo-random number generation algorithm [15] developed by Neils Ferguson and Bruce Schneier [16]. By using this cryptographic secure pseudo number generator a symmetric AES-key will be generated [16]. This key will then be used for data encryption according to the encryption concept.

C. Challenges Coming Along with the DLS

The main issue by taking this approach is that it relies on implementing a system to generate the CSV-response files by the data providers, which prevents them from buying or using already in place software, e.g. according to the ETSI standards.

Furthermore, the client-side code is provided to the participants by the DLS. This effectively means the DLS must be completely trusted. The DLS could selectively send down java script with encryption functionality completely disabled, or the DLS could provide the wrong public keys. While the client is audited, the public keys are certified, and a website exists with certificate fingerprints, it takes expertise to ascertain given and used certificates, as well as the client. Therefore, we advise to additionally use methods to ensure the integrity of the client and the certificates, as presented by Popa *et al.* [17].

VI. CONCLUSION

The Austrian legislator obviously has managed to implement the directive under conditions as little invasive as possible in respect of data privacy and legal protection aspects, by introducing technical, organizational and procedural countermeasures. For the implemented encryption scheme the data sovereignty stays with the communicating partners, as third-parties capturing the encrypted data are not able to have insight to any content. By

[6] https://www.bsi.bund.de/

DOI: 10.978.819252/12219

Downloaded from www.edlib.asdf.res.in

using strong cryptography, coping government satisfying authentication and security regulations, all communications are subject to certain general principles. For all Internet connections, a transport encryption is in any case provided. In addition, inquiries from authorities and the answers by providers must be encrypted (content encryption). Requests and responses can only be received and decrypted and thus viewed individually by each designated recipient. The DLS (or its administrators) cannot have insight to exchanged data and therefore confirm the blind concept, as the encryption and signing of data is done prior to the submission to the DLS. The Provider shall ensure that it provides the necessary data by business case. The DLS itself cannot take substantive control function here. The log data do not require data encryption. However, they are transferred to the DLS by means of transport encryption. The DLS can read log data and store it accordingly in its database. The system as a whole practically prevents setting unauthorized inquiries, by establishing transparency on the data exchanged and proves accountability of taken actions. Although, the European Court of Justice declared the Data Retention Directive invalid, we believe that the DLS system will be able to easily adapt to upcoming legal and political changes. The concept of the DLS has been time-proven with similar systems emerging[7] [8], and can easily be customized to be used for any sensitive data exchange between government authorities, as well as the economy. Future improvement should focus on implementing facilitative integrity controls and advanced cryptography in order to enhance the level of security and performance.

REFERENCES

[1] G. Black, "Publicity Rights and Image: Exploitation and Legal Control". Hart Publishing Limited, 2011.
[2] H. Rensen and S. Brink, "Linien der Rechtsprechung des Bundesverfassungsgerichts: erörtert von den wissenschaftlichen Mitarbeitern.", De Gruyter Recht, 2009, no. Bd. 1.
[3] Spiegel Online (2010), "Grundsatzurteil: Vorratsdatenspeicherung verstößt gegen Verfassung", [Jan 14, 2013].
[4] A. Meister (2012), "Vorratsdatenspeicherung in Tschechien verfassungswidrig, schon wieder", Netzpolitik.org, [Jan 07, 2013].
[5] L. Pimenidis and E. Kosta, "The impact of the retention of traffic and location data on the internet use", Datenschutz und Datensicherheit, vol. 32, pp. 92–97, 2008.
[6] G. Quirchmayr and C. C. Wills, "Some thoughts on the legal background of the continuously increasing privacy risk in information systems and on how to deal with it," in Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on, 2010, pp. 240–244.
[7] N. Vrakas, C. Kalloniatis, A. Tsohou, and S. Lambrinoudakis, "Privacy requirements engineering for trustworthy e-government services," in Proceedings of the 3rd International Conference on Trust and Trustworthy Computing, ser. TRUST'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 298–307.
[8] J. Vaidya, "Privacy in the context of digital government," in Proceedings of the 13th Annual International Conference on Digital Government Research, ser. dg.o '12. New York, NY, USA: ACM, 2012, pp. 302–303.
[9] S. Haryadi and I. Malik, "Lawful interception data retention regulation recommendation: Recommendations for countries that do not have relevant regulations of this field," in Telecommunication Systems, Services,and Applications (TSSA), 2011 6th International Conference on, Oct 2011, pp. 81–85.
[10] European Union, "Directive 2006/24/ec of the european parliament and of the council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks," in Official Journal of the European Union, 2006.
[11] C. Tschohl, "Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich," Ph.D. Dissertation, University of Vienna, Oct. 2011.
[12] L. Feiler and A. Stahov, "Die Einführung der Vorratsdatenspeicherung in Österreich," Medien und Recht, pp. 111–115, 2011.
[13] Bundesamt für Sicherheit in der Informationstechnik, "Technische Richtlinie BSI TR 02102-1 kryptographische Verfahren: Empfehlungen und Schlüssellängen," 2014.
[14] R. McEvoy, J. Curran, P. Cotter, and C. Murphy, "Fortuna: Crypto- graphically secure pseudo-random number generation in software and hardware," in Irish Signals and Systems Conference, 2006. IET, 2006, pp. 457–462.
[15] N. Ferguson, B. Schneier, and T. Kohno, "Cryptography Engineering: Design Principles and Practical Applications". Wiley, 2011.
[16] Y. Dodis, A. Shamir, N. Stephens-Davidowitz, and D. Wichs, "How to eat your entropy and have it too – optimal recovery strategies for compromised rngs," Cryptology ePrint Archive, Report 2014/167, 2014.
[17] R. A. Popa, E. Stark, J. Helfer, S. Valdez, N. Zeldovich, M. F. Kaashoek, and H. Balakrishnan, "Building web applications on top of encrypted data using mylar," in Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation, ser. NSDI'14. Berkeley, CA, USA: USENIX Association, 2014, pp. 157–172.

[7] https://lavaboom.com
[8] https://protonmail.ch

DOI: 10.978.819252/12219

Downloaded from www.edlib.asdf.res.in