Data Security Design as a Cooperation Facilitator

Data Security Architecture for Information Systems of Safety and Security Organisations

Marko Hassinen[1], Maija Marttila-Kontio[2] and Niina Päivinen[2]
[1]Department of Research and Development, Emergency Services College, Kuopio, Finland
[2]School of Computing, University of Eastern Finland, Kuopio, Finland
marko.hassinen@pelastusopisto.fi,{maija.marttila, niina.paivinen}@uef.fi

ABSTRACT

Different Safety (such as Fire & Rescue) and Security (such as Police and Border Guard) organizations handle sensitive data and material both in office and in field work. Some of this data is sensitive, while at the same time there is a lot of public material that could and should be available outside these organizations. This paper discusses the obstacles in sharing both public and sensitive data between safety and security organizations as well as disseminating public data to the audience. To cope with the rather complicated legislation and to facilitate organisational interoperability in data system level, we have created an application architecture that in our opinion satisfies both the need for data security and access to the public data. Although the legislative approach is to the Finnish law, the fundamental regulatory ideology is quite uniform within the EU and we feel our approach can be utilized not only on the union level but in any freely democratic society.

KEYWORDS

Data Security, Confidentiality, Safety, Security, Command, Control, Public Authority Cooperation.

1 INTRODUCTION

New information and communication technology is making way to safety and security field work. With new ways of communicating and collecting information, field work of safety and security workers can be made both more productive and safe. Accurate and up to date information is a key element in decision making in the sometimes hectic and fast paced operational work.

Decision making in operational field work in both safety and security domains is based on situational awareness and situational picture. This picture is based on information gathered from various, disparate sources, both remote, and, on site. These same information sources are often used also in the day to day office work.

The field work also often produces significant amount of information that has to be not only stored, but also disseminated to various other organizations on the scene. As some of this information can be highly sensitive or classified, the role of data security becomes very important. At the same time there is a clear need to serve the information needs of press and other media, not to forget the large public in general.

An additional set of data security needs come from authority cooperation on data system level. The need for common situational picture among fire rescue, police and border control, just to mention some, is obvious, and, there is a large project working on this in Finland at the moment. As different authorities may have different postures as to how they see their sensitive data in terms of protection levels, it is clear that this creates needs for harmonisation. Furthermore, there are a number of actors on this field that do not have the status of an authority, namely several volunteer organisations in the field of search and rescue. These invaluable forces have to be kept in mind when developing data systems for safety and security field.

As can easily be noted, the users for which interoperable cooperation tools are crafted, is very heterogeneous both in their organisational cultures and legislative stance.

The Finnish legislation has taken the transparency principal in regard to official documents. This means that all information that the government of municipal offices create and possess is public and publicly available to anyone, unless there is a reason stated in the law that dictates otherwise. This means that for every piece of information that is declared confidential, there has to be regulatory statement in the law.

The laws that state which pieces of official data can be considered confidential are disparate and difficult for a human to keep in mind. Hence, information systems must help users to identify the pieces of confidential information among the public ones. Also, the responsibility to identify and mark confidential details is made on the person who creates the information. There can be some exceptions to this rule, usually stated by the organisational rules of procedure.

To cope with the rather complicated legislation and to facilitate organisational interoperability in data system level, we have created an architecture that in our opinion satisfies all of the organisational needs stated earlier. The rest of this paper discusses the engineering decisions and motivations behind them. Also, we try to elaborate some technical aspects and more theoretical background, not forgetting the actual problem that needs a solution.

2 NORMATIVE BACKGROUND

As stated earlier, the law encourages transparency in the actions of government and municipalities. When these organisations use the public authority that has been given to them, the citizens must have the means to observe and influence on the decisions made. This public monitoring is a powerful tool for ensuring that the public servants pursue public's best interest and stick to the law. It is a fundamental principle in the use of public authority that every decision must be based on the law. To enable this possibility of public monitoring, the law states that all official documents have to be public unless there is statute that declares a document confidential. Also, the right to obtain public documents is subjective, meaning that one does not need to justify a request for such a document or identify oneself. As the facts stated above come from the Finnish legislation, the principles are similar on the EU level. European Council Code of Good Administrative Behaviour (EC 2000) states, among other things: "*Where a member of the public requires information relating to a Commission administrative procedure, staff shall ensure that this information is provided within the deadline fixed for the procedure in question.*" Similarly, the Code states that data protection rules for personal privacy shall be respected.

2.1 Confidentiality vs. Publicity

The most influential law concerning the publicity of official documents in Finland is the act concerning the publicity of the actions of public servants, namely the Act on the Openness of Government Activities (Ministry Of Justice 1999/621). This act states the common publicity principle and also the kinds of documents the publicity principle applies to.

A very important part of the act is the part that states which kind of documents are to be kept secret. In most cases these are documents concerning national or regional security, containing private details about businesses, private persons, criminal investigations etc. Also, documents containing details of plans for protecting the general population in large scale emergencies, natural accidents and civil defence are included.

As the legislation thrives to enable the individual to monitor the public authority, it also tries to protect the individual and her privacy. The laws concerning health care state very strict privacy rules on personal information. Also, any knowledge about personal matters, like lifestyle, family life and home are to remain confidential. Clearly, to list all of the (even relevant) matters legislation states having the need for protected privacy is not possible in this article.

2.2 Classifications and Protection Levels

Normative documents (Acts, official guidelines) in Finland define a widely used 4 step protection level system for confidential information. Protection level 1 is most severe requiring stringent data protection measures, while level 4 is the least demanding. How particular piece of information is placed on one of these protection levels depends on the severity of consequences if that data would be disclosed to an unauthorized third party or used unauthorised. Table 1 summarises the definitions of each level. Note, that it is the responsibility of the person who creates the document or piece of information to evaluate these consequences and place the document on the protection level accordingly. Also, as stated before, there has to be a legislative rule (data protection statute) before the document can be declared confidential.

Table 1: Protection levels with guidelines for placing a document to a particular protection level.

Protection Level	Damage caused by unauthorised disclosure
1	Particularly serious damage to the public interest the data protection statute protects
2	Significant damage to the public interest the data protection statute protects
3	Damage to the public or private interest the data protection statute protects
4	Harm to the public or private interest the data protection statute protects

In conjunction with the protection levels, government agencies are regulated to use classifications of information in cases when sensitive information can be harmful for national security or it is relevant to international security. Table 2 summarized these classifications and how they correspond to the protection levels. Note that in this article, the word confidential does not refer to a classification of this type unless explicitly stated.

Table 2: Classifications for government or international sensitive information.

Protection Level	Classification
1	TOP SECRET
2	SECRET
3	CONFIDENTIAL
4	RESTRICTED

For our purposes, it is sufficient to use the data protection level definitions. In designing the data security approach we reduce the classifications to their corresponding protection levels, but also make sure that possible classification notations can be retained. This is done for interoperability purposes, so the data system can handle and store also classified information.

2.3 Applying legislative aspects to application security design

There is little in the legislation that indicates the type of data security measures that one should employ to fulfil the requirements. In Finland, there is an act named Government Decree on Information Security in Governmental Administration (Ministry Of Justice 2010/681). Unfortunately, the authors have not found an English translation of this act. However, the act defines a baseline for data security in governmental administration. This is called the Basic Data Security Level. As a rule of thumb, data systems with documents (information) that are either public knowledge or defined sensitive and placed on protection level 4, should fulfil the basic security level demands.

3 DATA SECURITY

Now, that we have covered the fundamental normative ground for sensitive data, we are ready to look into and define the requirements for data security measures that can provide desired security levels for each data protection level. Requirements for data security procedures for each protection level are not found so much in the legislative as they are in other normative documents, such as the National Security Auditing Criteria (KATAKRI, Kansallinen turvallisuusaudotointikriteeristö) in Finland. These criteria have been developed for government bodies as well as private enterprises that work with governmental bodies to give a common set of rules and guidance when implementing data systems and data processing facilities in general. In addition to the Basic Data Protection Level, there are also two higher levels, the Raised Data Security Level and the High Data Security Level (KATAKRI, 2011). Data Systems containing protection level 3 information should fulfil the requirements of the raised level, whereas protection level 2 requires the high level. This distinction is very important in systems that provide authority cooperation, as different organisations are bound to have different protection level data. To ensure genuine ability for cooperation, it is critical that users with various protection level credentials can use the same system within the boundaries of their clearances.

There are numerous standards and guidelines for implementing secure computing environments, or parts thereof. These include standards, such as ISO/IEC 27002 and PCI DSS, and guidelines, such as the OWASP. In addition, a number of national guidelines, VAHTI guidelines in Finland, are used. For the purposes of our design, we rely mostly on the KATAKRI, which incorporates most, if not all of the above mentioned. Due to the scope of this paper and the limited space, we have to skip any more thorough look into these standards.

3.1 Data Security Requirements

Having a situation where different officials with different organisational background have to share sensitive information places some non-trivial requirements on the data system. Adding the

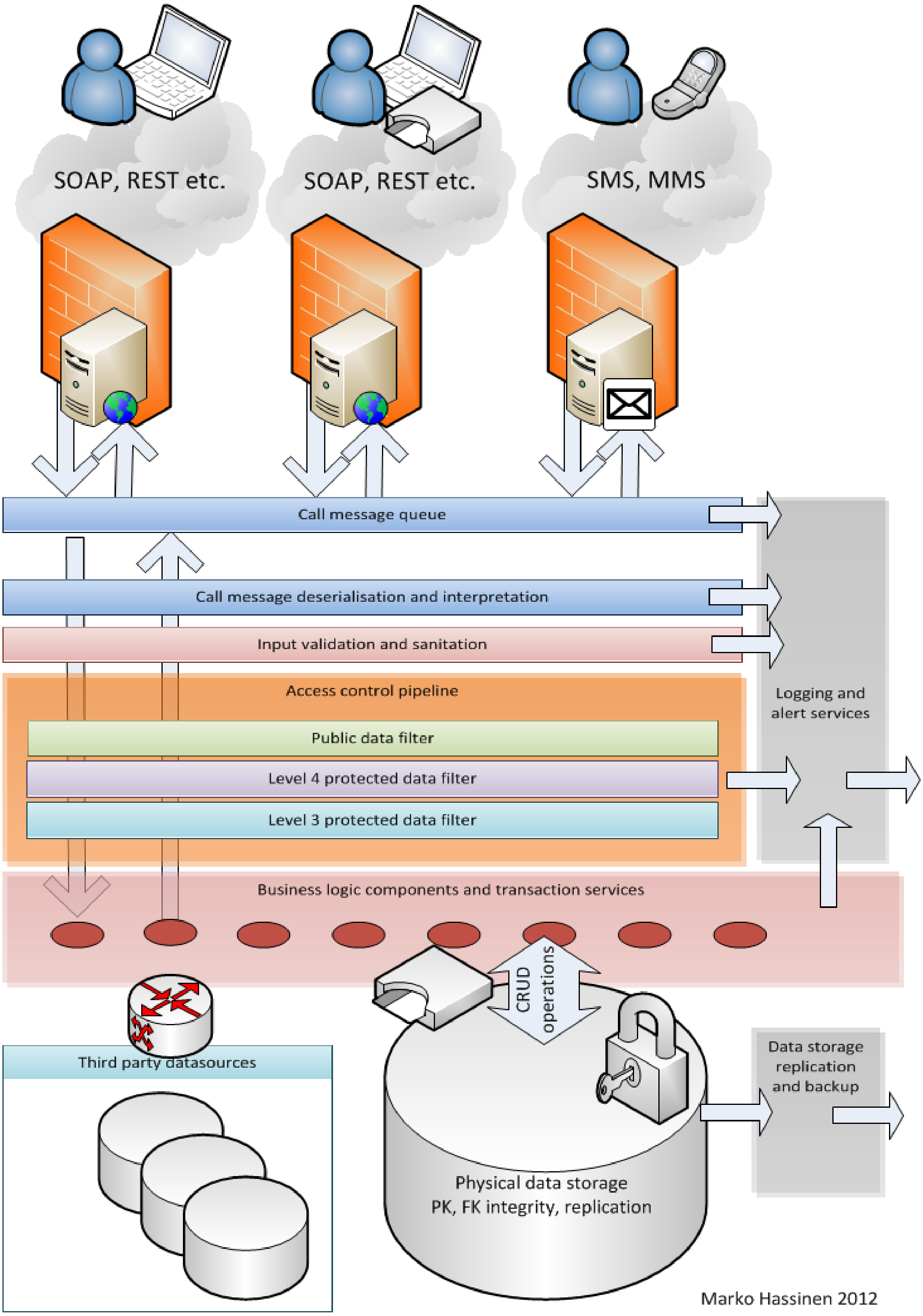
SOAP, REST etc.
SOAP, REST etc.
SMS, MMS
Call message queue
Call message deserialisation and interpretation
Input validation and sanitation
Access control pipeline
Public data filter
Level 4 protected data filter
Level 3 protected data filter
Logging and alert services
Business logic components and transaction services
CRUD operations
Third party datasources
Data storage replication and backup
Physical data storage PK, FK integrity, replication
Marko Hassinen 2012

Figure 1 Data security design for cooperative safety and security applications

ISBN: 978-0-9891305-0-9 ©2013 SDIWC

demand for freely available public data makes the situation even more complex. With these starting points we have crafted the most simple set of requirements we could think of. These requirements are:

1. Public data can be separated from sensitive, confidential data. The smallest such data element is a token, such as a word or a number etc,

2. System must be able to handle access for users with different access rights. A user with a right to access only public data must be able to read only public data. This is the no read up property of the common Bell-LaPadula model (Bell 1996). However, in some cases such user can write not only public data, but also data on a higher protection level. Obviously write here does not mean replace.

3. A user with access right to level 4 protected data can read data on protection level 4 and public data. Such user can also write level 4 data and public data. This is contradictory to the Bell-LaPadula model, hence we have not adopted it as is. In the model there is a no write down rule but it is not suitable for our case.

4. All read operations, except for reading public data, must have a valid need to know, meaning these actions must be relevant to the persons work tasks.

5. The access control must have flexibility and support work related roles. One person can be in more than one role over time.

4 SYSTEM ARCHITECTURE

To support the requirements stated in the 3.1, an application architecture that is based on a layered construct was defined. The architecture is drawn on figure 1.

The data is stored on a permanent storage that defaults to relational database, but can be anything, such as any NoSQL approach. We have considered such options as Hadoop (Hadoop, 2013) and MongoDB (MongoDB, 2013).

An important security consideration on the database is that it must remain confidential even if one could get the disk image of the server, hence, the database is encrypted using a smart card solution (The smart card cannot be stolen unless getting physical access to the server facility). The data storage replication uses this smart card as a token for mutual authentication with its remote counterpart.

The smart card is also a single point of failure in case the card malfunctions. This can be a common occurrence, as we have noted that smart cards tend to have a limited life span.

On top of the data storage is a layer that contains the business logic of the whole architecture crafted into atomic self-contained components that are designed to fulfil one task. This is a common component based programming paradigm solution, but in our focus is also security design in which a single component is responsible for a task that has a uniform access control requirement.

4.1 Access Control Pipeline

The core of the security architecture lies within the Access Control Pipeline. In essence it is a decision engine that uses the user role and identity to verify that the user has the right to perform a certain, requested operation. At the same time, it acts as a filter of data not letting any such data pass the filter that the particular user does not have access right to. Data is passed from the business logic to the pipeline in a structural form and views for the data are constructed only after the pipeline is done.

In order to support this decision making in the access control pipeline, we propose the use of ontologies. The security ontologies have been studied, for example, in the PoSecCo project (Basile, 2012). As we are defining a security system that has various levels of security, supports varying amount of user roles and provides flexibility in access control, the pipeline is a complex system. It seems ontologies can make the decision making somewhat easier. (McGuinness, 2004) Using the Web Ontology Language OWL, we can simply define the premises for access control decision making.

We already stated earlier that a person can have multiple roles which have different access rights. In order to support this kind of activity, we have adopted the operational role approach (Kurki, 2012). Operational roles are especially well suited to Safety and Security operational work, as these organisations and their workers are used to have hierarchical organisational structures with well-defined tasks for each role. However, the user role is not the only affecting factor, but also the circumstances under which the user has joined the data system. One of our design principles is that the user can be authenticated in several ways, such as a password based basic authentication or a strong two-factor authentication, such as, using a smart card token. Data security levels discussed earlier pose different requirements for the user environment. These include, but are not limited to, authentication mechanism (weak/strong), network from which the user traffic is coming (trusted/untrusted), and, the environment on the user device (hardened/regular).

In essence, even if the user by role has clearance for protection level 3 information and a valid need to know, the level 3 data is blocked at the filter if the user is not strongly authenticated.

The whole set of these rules is beyond the scope of this article and contains some elements that may themselves be sensitive information. The rule set itself forms basis for data security policy for a cooperative multi authority data system and can be used to create the Access Control Pipeline security ontology.

5 AGGREGATION

One of the most difficult things to handle with sensitive data is aggregation. Aggregation means a situation in which combining sensitive data creates a data set which is more sensitive than the individual pieces. Enforcing rules for these cases is not a trivial task, nor is identifying all such cases where aggregation may cause sensitive data to be disclosed to an unauthorized party.

In our architecture this problem is tackled with similar basic structure as the other access control pipeline decisions. Defining the forbidden data set combinations is manual labour, but it is done not by the user, but by the data security specialist in the software development phase. The access control pipeline keeps track of data elements a certain user has obtained and blocks access to elements that cannot be given to the user based on the history.

6 CONCLUSIONS

It is clear that official organisations that use public authority have to maintain certain transparency in their actions. To facilitate this transparency, the law governs that unless otherwise deemed sensitive by law, all information in these organisations is public.

In the process of supporting this transparency, we have developed an architecture for data systems that fine tunes the data storage to support both public data and access control for sensitive data. Using operational user roles we have been able to make a decision engine that supports existing organisational structures in the field work as well as in the office. With a very generic back-end design it is easy to provide different user interfaces to various end user needs and devices.

The cooperation of different public authorities, both governmental and municipal, and, also other organisations, requires a very flexible data security structure. Above mentioned actors have somewhat different readiness to handle data security requirements, and, are also obligated by different legislation. Our data security design can cope with these demands using an ontology based access control manager and data protection level filtering.

ACKNOWLEDGEMENTS

This work has been done in the close cooperation with and partly funded by projects TUPO, MoniKa and VARANTO of the Research and Development department of Emergency Services College, Finland. These projects are funded by the Fire Protection Fund, Palosuojelurahasto.

REFERENCES

European Council, 2000. *Code of Goof Administrative Behaviour*, Official Journal of the European Communities: OJ L 267, 20.10.2000

Ministery Of Justice : Act on the Openness of Government Activities (1999/621). http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf

Ministry Of Justice: Government Decree on Information Security in Governmental Administration (2010/681). In Finnish: http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Finnish National Security Authority (2011). National Security Auditing Criteria (KATAKRI) http://www.defmin.fi/files/1871/KATAKRI_eng_version.pdf

Bell, D. (1996). The bell-lapadula model. Journal of computer security, 4(2), 3.

Hadoop 2013. website: http://hadoop.apache.org/

MongoDB 2013, website: http://www.mongodb.org/

Basile C. (2010). Security Ontology Definition

McGuinness, D. L., & Van Harmelen, F. (2004). OWL web ontology language overview. W3C recommendation, 10(2004-03), 10.

Kurki T., Sihvonen H., 2012. *A Role-Based Resource Management Approach for Emergency Organizations* (PDF). Proceedings of the 45th Hawaii International Conference on System Sciences.

Official Journal of the European Communities: OJ L 267, 20.10.2000