Secure Distributed Dossier Management in the Legal Domain

Martijn Warnier Frances Brazier
Intelligent Interactive Distributed Systems
Faculty of Sciences, VU University Amsterdam
{warnier,frances}@cs.vu.nl

Martin Apistola Anja Oskamp
Computer Law Institute
Faculty of Law, VU University Amsterdam
{m.apistola,a.oskamp}@rechten.vu.nl

Abstract

The use of digital dossiers in Courts of Law, although currently in the phase of study, will be common practice in the future. This paper introduces the notion of distributed digital dossiers *supported by a multi-agent system architecture, developed in interaction with the Courts of Amsterdam and Rotterdam. Management of such dossiers is core to the approach: consistency, completeness, integrity and security key concepts.*

1. Introduction

In today's society information is inherently distributed across different physical locations and systems (both human and automated). More and more information is becoming available digitally, making it possible for information to be sought, structured, and processed electronically. This also holds for Courts of Law. Many sources of information are consulted during the course of a case. The Courts of Rotterdam and Amsterdam are currently experimenting with the digital dossier during trials. This dossier, prepared by the Public Prosecutor, is shared by the judge(s) involved, the public prosecutor, the defense and the clerks[1]. Each of these individuals can make his/her own notes and decide whether and with whom to share his/her notes.

The Public Prosecutor is responsible for the creation and preparation of the digital dossier. Although currently the dossier is based on scanned documents, more and more information (relevant for the dossier) is available electronically. This paper explores the options of *distributed digital dossiers*, supported by a multi-agent system architecture, to improve consistency, completeness, integrity and security of the information in such dossiers. This is also the goal of the the Agent-based Criminal Court Electronic Support Systems (ACCESS) project[2], initiated by the VU University Amsterdam together with the Courts of Amsterdam and Rotterdam, and financed by the Dutch Court for Jurisdiction[3] and NWO[4]. The focus of the project is on completeness, consistency, security and reliability of digital dossiers.

In our approach, physically distributed information sources, such as the Public Prosecution, the Police or the Prison system remain responsible for the integrity of their own information content, each monitored by one or more of their own software agents. The Public Prosecutor, in turn, is responsible for consistency and completeness of the dossier. Checks can be done periodically or whenever information is modified. Security is the topic of Section 2 together with the domain specific requirements of this application. Section 3 sketches how a distributed digital dossier can be implemented. Section 4 proposes the high level functional design of an agent based system for accessing the distributed digital dossier and Section 5 discusses the associated security architecture. Section 6 uses a simplified case study dealing with juvenile repeat offenders to illustrate some of the legal challenges of a system used in the environment of the courts. The paper ends with conclusions and future work.

2. Security requirements

The two most important requirements for the distributed digital dossier addressed in this paper are security and re-

[1] Defense lawyers are at the moment not included in this pilot study, but they should be at a later stage.

[2] http://www.iids.org/access

[3] Dutch: Raad voor de Rechtspraak

[4] the Netherlands Organization for Scientific Research

liability. These two requirements mandate more specific security requirements (1) that hold for all comparable distributed computer systems, but also (2) requirements that hold for this specific application, e.g. a judge should only have access to the cases with which he/she is directly involved. Personal dossiers may not be aggregated.

Nine principals, related directly to relatively standard security requirements for distributed clinical information systems [2] can be applied to the the Courts as follows:

1. *Access Control*: each individual dossier shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the access control list from accessing the dossier in any way.

2. *Dossier creation*: a dossier is always created by a public prosecutor.

3. *Control*: separate records in the dossier are the responsibility of individuals that are on the access control list. This person (possibly acting on behalf of an organization) is responsible for the record's information until at some later time the control is transferred to another person on the access control list.

4. *Notification*: defendants shall be informed of the content of the dossier as required by law. In some cases a defendant has the legal right to decide if information is added to a dossier. Defendants have the right to challenge the correctness of the information contained in the dossier during trial.

5. *Persistence*: no one shall have the ability to delete (parts of) the dossier, unless this is mandated by the (Dutch) law because the time for enforcement has passed (extinguishment).

6. *Attribution*: all changes to (records of) the digital dossier shall be marked with the subjects (users/organizations) identity as well as date and time. An audit trial must also be kept of all deletions[5].

7. *Information Flow*: information from record A may be appended to record B if and only if B's access control list is contained in A's.

8. *Aggregation control*: there shall be an effective measure to prevent the aggregation of personal information contained in the digital dossier.

9. *Trusted computing base*: computer systems that handle digital dossiers should have a subsystem that enforces the above principles in an effective way.

[5]For our purpose attribution and auditability can be regarded as similar requirements.

In addition, in the specific context of the digital dossier the following additional requirements hold:

10. *Secure transfer*: the (physically) distributed organizations shall only exchange information over secure communication channels that guarantee confidentiality and integrity of the transferred data.

11. *Compartmentalization of information*: it shall be possible for organizations to access only those parts of the dossier that they are responsible for and/or need access to.

12. *Consistency*: the data in the dossier shall be (internally) consistent.

13. *Completeness*: each dossier shall be complete when it is send to the court and lawyers of the defendants.

14. *Backups*: periodically backups of each dossier shall be made. These backup copies are secured against unauthorized access in a similar fashion as the original dossiers.

Consistency and completeness are especially challenging requirements: they must be guaranteed. When an authorized organization, e.g. the Council for Child Defence, adds a record to a specific digital dossier, the system needs to check whether the information is *consistent* with all other information in the dossier, for example whether e.g. personal information, such as name, address, age and sex of the subject, is consistent across records/documents.

Completeness requirements hold for all dossiers including generic completeness requirements, and offense specific completeness requirements. Generic completeness requirements specify that certain personal information on the defendant as well as the offense for which the defendant is charged, and the official report filed by the police, must be included. In addition, offense specific completeness requirements hold: e.g. a drunken driving charge requires an alcohol test by an authorized lab. The system should guarantee completeness of the dossier before it is transferred to the Court.

The next sections propose a design for an agent based support system for the distributed digital dossier that fulfills the above mentioned requirements.

3. The distributed digital dossier

The nature of the application with physically distributed sources of information distributed over different organizations is the reason this paper proposes a *distributed digital dossier*. This section describes the implications for the organizations involved.

Each individual digital dossier is created by the Public Prosecutor once he/she decides, on the basis of information available, to prosecute a defendant. A newly created dossier consists of records and meta data. The meta data contains information such as the access control list for this dossier, logging information on who altered or accessed information at what time and when the last backup of the dossier was made. The meta data part of the dossier is stored by the the Public Prosecution.

Individual records are the responsibility of different organizations. Personal information, for example, is managed and maintained by the defendant's local authorities. Information on a juvenile's family situation is provided by the the Council for Child Defence etc.. Distributing this data and the responsibility for the data ensures that information in the digital dossier is kept as up-to-date as possible. Changes in data are flagged by the relevant organizations and transmitted to the the Public Prosecution for synchronization of the complete (distributed) dossier.

Thus the basic dossier itself is stored by the Public Prosecution while relevant records are maintained and stored by the responsible organizations and then synchronized with the digital dossier by the the Public Prosecution.

When the the Public Prosecution decides that a case is ready for Court the dossier is 'frozen': the dossier is finalized and forwarded to the presiding judge and the defendant's lawyer. From this point on the dossier is no longer distributed and other organizations are no longer responsible for "their" records. Note that as a result a trial is based on information available at this point in time.

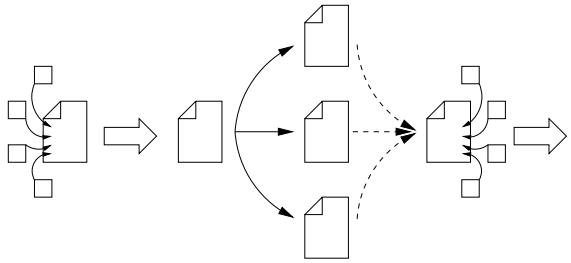
As is currently the case, the the Public Prosecution decides which information is included in the frozen version of the dossier, and which not, based on his/her judgment of its relevance. Additional information can, from this moment on, only be added by one of the parties involved by special procedure that ensures that the relevant additions to the dossier are distributed to the concerned parties (prosecutors, judges and defense lawyers).

Once a case has been tried, a dossier can be 'defrosted', i.e., made distributed again, re-'frozen' when needed for a trial, etc. This process can be repeated numerous times (retrials, appeals etc.) until a dossier is finally closed.

Management of this process can be based on one of Two life cycle models for digital dossiers:

- *The naive life cycle model*, is the conceptually most straightforward model. A dossier is 'frozen' (static and centralized) and 'defrosted' (dynamic and distributed) as required. Note that a technical solution for defrosting a dossier is non-trivial, as it requires identification of the appropriate organization for each record in the dossier and complete new resynchronization of information contained in the dossier's records. Doing this automatically is a challenge.

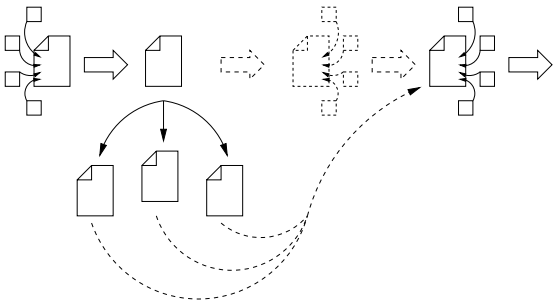
  The picture below illustrates the naive model:

  A *distributed digital dossier* is shown on the far left. This dossier is frozen, resulting in a static file with the current state of the data. Next, as indicated by the solid black arrows copies of this static dossier are distributed to the Public Prosecution, the Court and the defendant's lawyer. If a new trial is needed, e.g. due to a miss-trial or an appeal, the dossier is distributed again (defrosted), as shown on the far right of the picture. Each organization is again responsible for "its" records in the dossier.

- *The semi-freezing life cycle model*, is less drastic. Freezing entails making a local central copy of the dossier as in the above case. The difference is that the distributed version of the dossier still exists. If and when a dossier is defrosted, a new version is instantly available (again). This model is technically preferable, the only difficulty that can arise is that during trial, additional information may have been added to the dossier (by the Court or the defense). This information needs to be distributed to the relevant parties. By default the Public Prosecution is responsible for this information.

  The semi-freezing model is schematically displayed below:

  As in the naive model, the *distributed digital dossier* is shown on the far left. Once the dossier is frozen and copied (solid arrows), the dossier remains distributed (indicated by the dashed arrows). If and when a case

is directed to a new Court, a completely new dossier can be acquired on the basis of the information as known to the distributed organizations responsible for the records. New information that surfaced during the trial, however, needs to be incorporated into the rest of the distributed dossier.

Both models have technical and conceptual advantages. As the semi-freezing model ensures a maximum of both control and responsibility for all parties involved this model is preferred. As such it is used in the remainder of this paper. The next section illustrates how the distributed digital dossier can be supported by means of a multi-agent system. The proposed security architecture that fulfills the requirements from Section 2 is proposed in Section 5.

4. An agent based design

This section describes the functional design of a multi agent system for distributed digital dossier support. Note that no attempt is made to describe the exact type of information that is contained in each digital dossier. This information highly depends on the specific offense/crime involved, e.g. not all digital dossiers will contain a DNA entry type. All dossiers, however, do contain entry fields for information such as the personal information of the defendant.

Distributed multi-agent systems provide a promising paradigm for large scale distributed autonomous systems [7]. Agents are pro-active, adapt to a changing world and can be mobile [16]. The main reasons for using an agent system is a conceptually clear model for autonomous systems that supports modularity, security and scalability. Specific tasks can be implemented by dedicated agents, allowing for a clear separation of concerns and straightforward integration of new functionality as new agents.

¿From a technical perspective, one or more computer hosts that are maintained by the same organization together form a *location*. A dedicated middleware layer, the *agent platform* ensures that all hosts at a location can be viewed as one logical unit. The middleware ensures that all agents can uniquely be identified (using a lookup service), that agents on different locations can communicate with each other and that, if required, agents can migrate between locations[6]. Examples of such agent systems include AgentScape [8], JADE [3] and SeMoA [10].

In our model all interaction with the digital dossier is facilitated by means of agents. Only authorized agents can alter records in a dossier. The dossier is the single point of entry, providing a means to regulate access control (see the next section).

[6]Not all agent systems allow migration of agents.

Each functional organization has its own collection of hosts (agent location) and an agent platform. This allows *local control* and responsibility of data (and access to data) while at the same time it supports the use of *global security policies* that can guarantee a minimal set of (global) security requirements. The next section elaborates further on this topic.

5. Security architecture

The following security architecture provides a means to fulfill the security requirements identified in Section 2.

The semi-open nature of the environment of the Courts makes access control a particular challenge. Access control regulations in such systems generally tend to make *all* data more difficult to access, including the less sensitive information that can be of interest to a large public. This phenomenon is known to as 'label creep' in the literature [11].

Our proposed solutions handles this problem by means of a two-tier access model. On the first level role based access control [12] is used as an access control mechanism for access to the information system that contains the distributed digital dossier. Each 'role', such as a judge, a lawyer, the Public Prosecution, or a clerk, has certain rights regarding the dossier. This will depend on specific security policies, e.g. a clerk may only add information to the dossier, not delete or modify anything, while the Public Prosecution may change existing information in the dossier and even create new dossiers.

Additionally, the second access level uses access control lists [6] to limit the access of individuals. Each dossier contains (in its meta data) information on specific individuals that may change, read, delete or add information to a dossier. For example, judge A may read a specific dossier (since its his/her case), while judge B may not. Thus in order to change records in the digital dossier (via an agent) the user also has to be on the access control list of a specific dossier.

The distinction between roles and individuals is crucial in a dynamic environment (such as is the case associated with the digital dossier). Security policies based on roles can be regarded as static (or at least 'long lived') and are typically globally valid (at all possible locations), while individual access control lists are typically dynamic (or 'short lived'). Individual policies typically only apply per dossier, or even shorter if a dossier is handed over to another clerk/prosecutor/judge etc. The combination of static and dynamic access control rules should also limit the 'label creep' phenomena.

In addition, each user also has a public/private key pair and a corresponding digital certificate, as specified in the X509 standard [1]. The certificates are organized in a standard PKI infrastructure [6] and are used for signatures on

individual records, to enforce integrity of a digital dossier as a whole.

Other security requirements are handled by the agent platform [15]: integrity of agents and their data, secure communication (and possibly migration) between platform locations (e.g. Public Prosecution Services and the Council for Child Defence) etc. All other functionality, including security, are implemented by individual agents. These include, amongst others, the following:

- *Completeness*: A dedicated agent checks the completeness of each dossier. A dossier should always include the required minimal information such as personal information, criminal charge and warrants. Additional completeness checks are performed on a per case basis. For example, a dossier concerning a drunk driving case should include a rapport that details the factual information of the alcohol blood level at the time of the offense.

- *Consistency*: Consistency is checked whenever information from an outside source (such as from the Council for Child Defence) is entered in the digital dossier. A dedicated consistency agent (per dossier) checks if all personal data from the outside source matches the data in the digital dossier. If this is not the case a (human) agent needs to decide how to act further. The consistency agent will mark such an event in the meta data of the digital dossier. It is also possible for the agent to make an 'educated guess' related to (simple) consistency issues. This can automate parts of resolving consistency problems. Though notice that (external) consistency cannot be guaranteed automatically, since the agent needs to confirm the reliability of the information it has with outside sources, something that is usually not possible.

- *Persistence*: Dedicated agents guard the life of data entries in the digital dossier. For example, information obtained from the Council for Child Defence concerning juvenile suspects may, by law, only be kept for a maximum period of five years and should also be destroyed when the subject turns 18.

- *Attribution*: A logging agent is responsible for logging all information per dossier (who changed what, when, etc.). This information is safely stored (preferably offline and encrypted) and needs to be integrity preserving (using signatures).

- *Backups*: Similarly, a special purpose backup agent can be deployed to facilitate secure backups of the digital dossier. This could be combined with the logging agent, since these agents share a lot of functionality.

This system is inherently modular, new functionality can be added by new agents that can be used whenever required. For example, an agent that can advise a judge about the strictness of a verdict in similar cases can be integrated in the agent system without any difficulty.

6. Legal issues

The example of juvenile repeat offenders is used in this paper to illustrate the types of information included in a distributed digital dossier and their sources, the focus is on the information exchange between the Public Prosecution and the Council for Child Defence. This scenario has been chosen because repeat offenders and especially juvenile offenders represent an interesting and socially important subject. If it is possible to reduce the number of juvenile repeat offenders, identify responsible parties in an earlier phase and/or stream-line the trial chain associated with juvenile repeat offenders in any way then the gains can be huge.

A fictive scenario is presented to illustrate a number of legal issues in relation to the use of agent technology in a criminal trial, in a Dutch legal setting[7]. In this scenario an agent of the Public Prosecution requests (an agent of) the Council for Child Defence to add information regarding a child's (a juvenile suspect) home environment to the digital dossier. If successful, the Council for Child Defence's agent adds the newly acquired information regarding the child's home environment to the digital dossier. A signature, using the Council for Child Defence's private key, over the newly created record is also included in the dossier. If the the Council for Child Defence does not wish to provide this information the Council for Child Defence's agent adds a note that the information was requested but not released. The reason why the information was not released is provided, e.g. because the Council for Child Defence did not have this information or was unwilling to provide the information for a specific reason, etc. Note that security requirements such as persistence and attribution are of importance.

More precisely, the scenario requires an agent of the Public Prosecution to send a message to the agent of the Council for Child Defence requesting information regarding the child's home environment of a juvenile defendant. All personal data of the defendant is contained in the message to minimize the risk that the wrong information is added to the digital dossier of the defendant's case. At the Council for Child Defence an agent checks if there is a file of the defendant. If this is indeed the case then the relevant information (concerning the child's home environment) of the defendant is sent back to the the Public Prosecution and added to the

[7]Note that in this paper all legal and procedural details are interpreted in the context of Dutch law. For most situations sketched it should be clear how the situation can be modified for other legal domains. Unlike in most countries the Dutch legal system does not know jury trial.

defendant's digital dossier. If the information cannot be released this is reported back to the agent of the Public Prosecution along with the reason. This negative answer is also stored in the digital dossier.

From a legal perspective it is important for the Public Prosecution and the Council for Child Defence to know to whom an agent belongs, as it acts on behalf of this person/organization [5]. Identification is also important when dealing with liability and compliance with agreements. From a legal perspective it is not possible to hold software agents themselves responsible for any actions. The owner/user is always responsible [13]: there must be a link between the agent and its provider or user (attribution).

Taking into account the responsibility of the Public Prosecution and the Council for Child Defence for their agents and the aim and execution of the tasks of the Council for Child Defence, and the reports of the Council for Child Defence, the agent of the Public Prosecution can request reports from the agent of the Council for Child Defence, that is, reports concerning advices, petitions and counseling in criminal cases [14]. Before adding personal data to a digital dossier, the Council for Child Defence needs to justify such a decision. Only if the client (the defendant) of the Council for Child Defence gives explicit permission to exchange his/her own personal data, can (the agent of) the Council for Child Defence supply the personal data to the agent of the Public Prosecution (notification). The Counsel for Child Defense may also supply information to the agent of the Public Prosecution when there is a legal duty to do so or when supplying information is necessary for a good execution of the Public Prosecution's tasks. As a guideline, Dutch law forbids the exchange of certain personal data, unless there is a legal valid reason. In all cases in which the Council for Child Defence is legally allowed to release personal data for the digital dossier, it needs to inform that person of its action. The Public Prosecution Service is expected to carefully handle the received reports to guarantee the privacy of the client of the Council for Child Defence. The Counsel for Child Defense must add a record to the (local) dossier of their client that states, when and to whom what data was supplied.

The Public Prosecution Service can only give information to the Council for Child Defence when necessary for a good execution of the tasks of the Public Prosecution and insofar a weighty public interest is involved. This last criterion is for protection of others [4]. Furthermore, giving information to the Council for Child Defence must serve a purpose as stated in legislation. In the case of possible child abuse or other domestic violence in which children are victims, the purpose may be preventing criminal acts or supporting victims. In that case information can be given to the Council for Child Defence. For the preparation of dossiers the Minister of Justice may give copies of reports in personal dossiers to the director of the Council for Child Defence.

This small scenario illustrates that provided with a clear security architecture digital dossiers and agent technology can be used to fulfill legal requirements on information exchange and management. More research will give a more complete overview of legal requirements, also for other cases.

7. Conclusions

A distributed digital dossier in combination with a multi-agent system that is used to access and secure the dossier can provide major benefits for an information management system in the legal environment, specifically the Courts.

The main requirements for such a system are consistency, completeness, reliability and security in the form of access control, confidentiality and integrity. The proposed system for the distributed digital dossier in the Court of Law adheres to all these requirements.

Other requirements, such as scalability and performance, have not been studied. Though state of the art hardware can usually fulfill such requirements, e.g. if a location does not handle requests of users (and agents) fast enough, additional hosts can be added to an agent platform location and an optic fiber-tube connection between the Public Prosecution and the Council for Child Defence can help minimize slow network connections.

8. Future Work

The agent based security architecture presented in this paper is only the starting point for an information management system for a Court of Law. Numerous issues remain. Our current research focuses on handling consistency and completeness of digital dossiers automatically. The first results, employing AI techniques, look promising, but still require additional effort. On the legal side, the Dutch situation needs to be compared to the situation in other countries and legal systems.

A first prototype of the system proposed in this paper is currently under development. The agent platform Agentscape [8] is being used to realize this system.

Acknowledgment

This research is supported by the NLnet Foundation, `http://www.nlnet.nl`, and is conducted as part of the ACCESS project, `http://www.iids.org/access` funded by the NWO TOKEN program.

References

[1] C. Adams and S. Farrell. RFC2510: Internet X. 509 Public Key Infrastructure Certificate Management Protocols. *Internet RFCs*, 1999.

[2] R. Anderson. Clinical System Security – Interim Guidelines. *British Medical Journal*, 312:109–111, 1996.

[3] F. Bellifemine, A. Poggi, and G. Rimassa. JADE–A FIPA-compliant agent framework. *Proceedings of PAAM*, 99:97–108, 1999.

[4] M. Bruning. *Over sommige kinderen moet je praten*. Universiteit Leiden, 2006. Oratie.

[5] L. B. B.W. Schermer, M. Durinck. Juridische aspecten van autonome systemen. Technical report, ECP.NL, 2005.

[6] C. Kaufman, R. Perlman, and M. Speciner. *Network Security, PRIVATE Communication in a PUBLIC World*. Prentice Hall, 2nd edition, 2002.

[7] M. Luck, P. McBurney, and C. Preist. *Agent Technology: Enabling Next Generation Computing (A Roadmap for Agent Based Computing)*. AgentLink, 2003.

[8] B. Overeinder and F. Brazier. Scalable middleware environment for agent-based internet applications. In *Proceedings of the Workshop on State-of-the-Art in Scientific Computing (PARA'04)*, volume 3732 of *Lecture Notes in Computer Science*, pages 675–679, Copenhagen, Denmark, June 2004. Springer.

[9] W. Rankl and W. Effing. *Smart Card Handbook*. John Wiley & Sons, 2nd edition, 2000.

[10] V. Roth and M. Jalali-Sohi. Concepts and architecture of a security-centric mobile agent server. In *"Proc. of the Fifth International Symposium on Autonomous Decentralized Systems (ISADS 2001)"*, pages 435–442. IEEE Computer Society, 2001.

[11] A. Sabelfeld and A. C. Myers. Language-Based Information-Flow Security. *IEEE Journal on selected areas in communications*, 21(1), 2003.

[12] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-Based Access Control Models. *Computer*, 29(2):38–47, 1996.

[13] B. Schermer. Handreiking voor gedragsregels autonome systemen. Technical report, ECP.NL, 2006.

[14] M. van Justitie. Normen 2000. beleidsregels met betrekking tot de werkwijze van de raad voor de kinderbescherming. Technical Report Versie 2, Directie Jeugd en Criminaliteitspreventie, 2000.

[15] G. van 't Noordende, F. Brazier, and A. Tanenbaum. Security in a mobile agent system. In *Proceedings of the First IEEE Symposium on Multi-Agent Security and Survivability*, Philadelphia, 2004.

[16] M. Wooldridge and N. Jennings. Intelligent Agents: Theory and Practice. *The Knowledge Engineering Review*, 10(2):115–152, 1995.