REDUCE THREATS IN COMPETITIVE INTELLIGENCE SYSTEM: A GENERIC INFORMATION FUSION ACCESS CONTROL MODEL

Anass El haddadi1, 2, Hamid Hatim2, Bernard Dousset1, Ilham Berrada2, and Hanane El Bakkali2
1IRIT UMR 5505, Toulouse University 3, Toulouse, French
haddadi@irit.fr , dousset@irit.fr
2ENSIAS, Al BIRONI Team, Med V University, Rabat, Morocco
hamidhatim@yahoo.fr , iberrada@ensias.ma , elbakkali@ensias.ma

ABSTRACT

Information fusion is a cornerstone of competitive intelligence activity that aims at supporting decision making by collecting, analyzing and disseminating information. This information comes from heterogeneous data sources. In this paper we present an approach of access control. This approach is focused both on the information that must be bring to decision-makers and the privacy of individuals whose data is used to extract this information. This model is based on the standard "Role Based Access Control" (RBAC) and is implemented within the entire life cycle of Xplor Every Where (Web service of Tetralogie), it follows methodologies tailored to design privacy-aware systems to be compliant with data protection regulations.

KEYWORDS

Competitive Intelligence, Access Control, Data Security, Process Security, Tetralogie, Xplor Every Where

1. INTRODUCTION

Competition is a fundamental concept of the liberal economy tradition that requires companies to resort to competitive intelligence (CI) in order to be advantageously positioned on the market, or simply to survive. Nevertheless, it is well known that it is not the strongest of the species that survives, nor the most intelligent, but rather, the one most adaptable to change, the dominant factor in society today.

Therefore, companies are required to remain constantly on a wakefulness state to watch for any change in order to make the appropriate solution in real time. However, for a successful vigil, we should not be satisfied merely to monitor the opportunities, but before all, to anticipate risks. The external risk factors have never been so many: extremely dynamic and unpredictable markets, new mergers and acquisitions, sharp price reduction, rapid changes in consumption patterns and values, fragility of brands and their reputation.

DOI: 10.5121/ijdms.2011.3102

To face all these challenges, competitive intelligence system (CIS) where designed to provide online services. CI is both a process and a product [1]. As a process, it is the set of legal and ethical methods a company uses to harness information that helps it achieve success in a global environment. As a product, CI can be considered as Information Fusion about competitors' activities from public and private sources, and its scope is the present and future behavior of competitors, suppliers, customers, technologies, acquisitions, markets, products and services, and the general business environment. It may include activities such as examining newspaper articles, corporate publications, websites, patent filings, specialized databases, information at trade shows and blogs, making privacy and data protection as pivotal issues, since they concern the right to prevent the dissemination of sensitive or confidential information of individuals [2].

The need for security in a CIS arises out of the strategic nature of information conveyed with quite a substantial value. Such security should not be considered as an additional option that a CIS can provide just in order to be distinguished from one another. Especially as the leak of this information is not the result of inherent weaknesses in corporate computer systems, but above all it is an organizational issue.

So the issue is how to protect both data (CI as a product) and treatments (CI as a process). Thus, our contribution in this paper is to propose an access control model of data and treatment in CI platforms so that all tasks are only executed by authorized users.

The rest of the paper is structured as follow: First, we identify in section 2 risks and vulnerabilities in CIS in order to express the needs for access control to data and information treatments. In section 3, we will explain privacy threats that arise when performing a CI activity. Section 4 presents our access control approach implementing on Xplor Every Where (XEW) CIS. This section describes the access control and privacy policy that are part of our access control model. Section 5 summarizes and assesses the approach.

2. RELATED WORK

In a CI platform a risk is the likelihood of a negative event multiplied by its impact [3]. The likelihood can be estimated based on assumptions about trust and about the underlying coordination model.

In 2008, a survey shows that 73% of companies with over 200 employees consider as dramatic the consequences of a failure within 24 hours of their information system [4]. This dependency on IT is particularly acute in the field of CI where all activities are fully automated monitoring nowadays.

As any Information fusion process [5], a CI platform activity either it is outsourced to a service provider or conducted internally takes place in several steps, each requiring a specific form of security. The first step, data collection, requires a security service in terms of availability, integrity and confidentiality [6]. Any data alteration in this level implies wrong predictions so that all the sense of CI is broken down. The second step, treatment of collected data, requires an access control service that implements an Authentication/Authorization service to restrict access only to mandated people to fulfill different tasks. Preservation of professional secrecy is an example of the importance of this step. Finally, the ultimate step, issuing of the information estimated as 'strategic' for the decision-maker, requires a mutual (platform/decision-maker) authentication service.

Security risks are even more important for a collaborative CIS, where watchers (the CI activity agents) are organized in networks to achieve collectively a CI activity by means of a forum. In this case, managing remote access right of users is really a laborious task, because in the majority of cases, the architecture of the network doesn't reflect the security policy [7].

Our solution is to provide a 'transparent' security system, because if it will be 'understandable' for the attacker (notice that understanding a security system doesn't necessarily mean detecting a vulnerability), before and after all, it will be understandable to the security administrator, a mandatory condition to stand guard.

Figure 1 shows some security issues and challenges that might affect the CIS. These problems are both external of the system (a malicious competitor attack for example) and internal (separation of duties between the different involved roles to avoid a conflict of interest, least privilege granted to each user to prevent him from going beyond his prerogatives, etc …) .

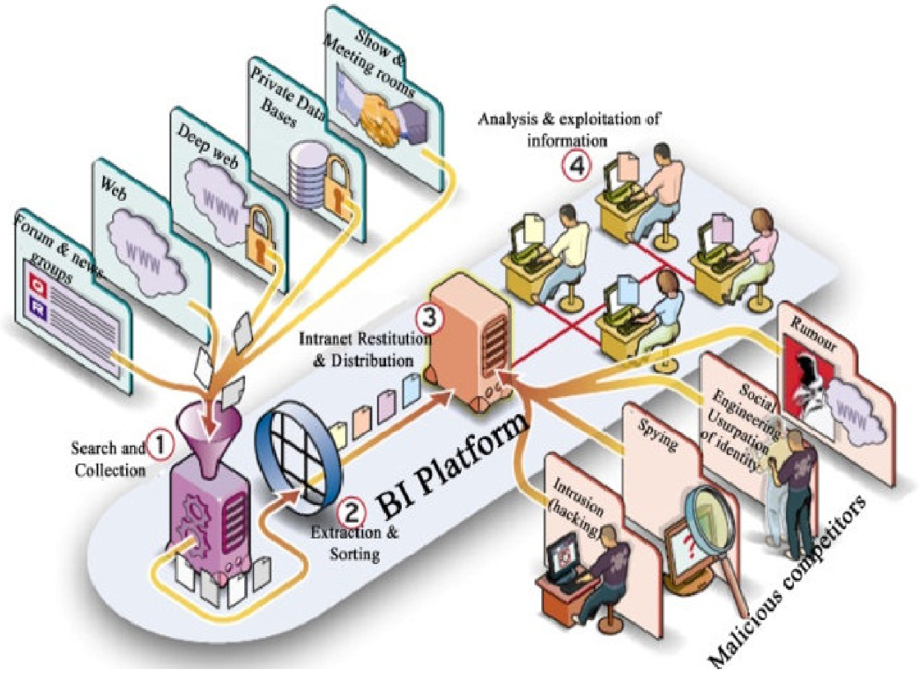


Figure 1. Interactions in a CI process [8]

3. SECURITY RISK AND VULNERABILITY IN A CI PLATFORM

3.1. Risks associated with Data importation: The outsider threats

Internet is the main Data sources of a CI monitoring activity. Any known search engine can Import these data by getting a copy of each indexed page from the visible web (forums, news groups, blogs, newsletters, intranets, RSS, Blog).

However, searching on the Internet today can be compared to dragging a net across the surface of the ocean; a large amount of information can be fished on the internet, but there is a wealth of information that is deep and therefore missed. Most of the Web's information is buried far down on dynamically generated sites, and standard search engines do not find it. Traditional search engines cannot "see" or retrieve content in the deep Web – those pages do not exist until they are created dynamically as the result of a specific search [9]. Therefore, specific tools (web crowlers for example) are purchased or developed at home to explore the deep web (online databases, sites that require registration and authentication, social networks, etc...). Several risks are related to data importation. They are characterized as outsider threats since they are located outside the CI platform.

3.1.1. Risks associated with the use of collection tools

Precautions must be taken when we integrate open source tools in our platform. We must ensure (by recompiling ourselves the code) that these tools are not in fact “malwares” intended to send back the analysis results of data they import. "You can’t trust code that you did not totally create yourself" [7]. Pirated software which might contain backdoors or malicious code must be forbidden.

3.1.2. Risks related to the data sources reliability

Some sites can’t be trusted to give accurate information and fail to provide the claimed services. To collect information only from reliable sources, we must rely on certificates from certification body that verifies among others that a web site has a good privacy policy. We must also ensure that the information is accurate, current and complete, including the relevant context in which it was sought or received; Examples of these threats are spoofing, impersonating other users, eavesdropping and packet sniffing.

3.1.3. Risks related to legal aspects

Competitive Intelligence is completely separate from espionage (That involves individual obtaining information that is considered secret or confidential without the permission of the holder of the information). The monitoring activity in a CI Process must be done in a lawful manner and a special attention must be paid to the preservation of privacy. In the USA, strategic and competitive intelligence activities are subjects of federal laws that explain among others, arrangements under which a watch can be conducted [10].

3.2. Risks related with treatment process and data analysis: The Insider threats

The annual CSI Computer Crime and Security Survey for 2008 found in its survey of 522 security employees from US corporations and government agencies that 44 percent of respondents cited insider incidents. Unlike outsider attacks operated by unauthorized users to access the system, insider threats and vulnerabilities are related to the misuse of privileges by properly authorized and identified users of the system. Indeed in many cases, formal security policies are incomplete and implicit or they are purposely ignored in order to get business goals accomplished. Even most recent studies estimate that no mechanism exists to prevent insider abuse [11].
According to [12], there seems to be little design and technology available to address the insider threat problem. However, many forms of attack have been reported:

- Unauthorized extraction, duplication, or ex-filtration of data;
- Tampering with data (unauthorized changes of data or records);
- Destruction and deletion of critical assets;
- Misuse of resources for non-business related or unauthorized activities;
- Purposefully or deliberately installing malicious software.

Once data are imported in a successful security way, we must prevent information leakage. In most cases, this last happens whenever a system that is designed to be closed to an eavesdropper reveals some information to unauthorized parties nonetheless. Since Information leakage can subtly or completely destroy the security, good Access Control mechanism must be designed to limit the privileges of each user just to fulfill the task corresponding to his job. No permission must be held unnecessary.

3.3. Risks related to information delivery: Both Insider & outsider threats

This step constitutes the core of a CI activity: Deliver the treatment and analysis outcome to the decision-maker. There are two ways to achieve this purpose:

• Pull strategy: The customer (decision-maker) will seek the information itself on the server. In this case, a web portal of the platform should provide the results after successfully authentication the client. The growth of electronic commerce in recent years has provided significant advances in security that can be reused in the internet portals platforms of CI.

• Push strategy: The server sends the information to the client as a message to his computer or his smart phone.

Our XEW uses the second strategy and so, it sends results to the client in his Smartphone. Smart phones, in general, were designed as open, programmable network devices that can provide various PC-like services, such as messaging, email, and Web browsing. As such, they're vulnerable to attacks that can compromise the confidentiality, integrity, and availability of data and service. They must be equipped with protection systems as SELinux [13] because henceforth, they are not only display devices but they contain critical information on which depends the success of the business. Di Pietro etV. Mancini [14] has illustrated how the user's privacy and security appears at risk under his Smartphone interoperability with other devices.

4. PRIVACY THREATS IN A CIS

Privacy is the ability of an individual or group to keep related information, their social and behavioral patterns out of public view, or to control the flow of information about themselves [15]. Privacy is often translated as confidentiality. In this paper, we stress privacy in its dictionary based meaning: the freedom of not having someone or something to interfere in our life without our permission [14]

CI platforms collect a vast amount of personal information from and about consumers. This information is routinely collected from consumers through registration forms, order forms, surveys, contests, and other means, and includes personal identifying information, which can be used to locate or identify an individual, and non-identifying information [16].

4.1. Motivation example

Suppose a telecommunication company that calls in a CI platform to maintain its customers through a marketing policy. The CI platform needs understanding the factors that determine a client's decision to remain in a cluster or leave for another. In order to give its predictions, The CI platform uses the following data about the company's customers : Age, sex, region, salary, married, number of children, having a car, credit, starting date of the credit, account-type, current balance , starting balance, opening date of the account etc … to discover co-occurrence relationships that influences loyalty programs. The large amount of transactional data may contain customer spending patterns and trends that are essential for marketing and planning purposes.

These data are related to the company's customers who bought a mobile phone from the company at a given moment. Customers provide information about themselves on the basis of trust. In its usual sense, trust is a social construct that has rich overtones of ethics, morality, and religion, but computers have no moral sense and rely only on computations [7]. So, the word "trust" applied to a computer is, in reality, trust in its designers, creators, and users.

It seems there is no problem of privacy since information is provided anonymously. However, this personal information may be considered as sensitive, due to the existence in the data of quasi-identifying attributes (QID), such as age, region (zip code), etc… [17]. An attacker can join the QID with external information, such as voting registration lists, to re-identify individual records.

4.2. Privacy preservation techniques

Traditionally, privacy enhancing technologies have been thought as tools for hiding, obfuscating, and controlling disclosure … in short, basing on anonymity. Nevertheless, four states of privacy are described in the literature: solitude, intimacy, anonymity, and reserve [18].

Jorns et all [19] uses transaction pseudonyms for the exchange of sensitive data by preserving user's privacy. Pseudonyms are used as identifiers that allows for anonymity in identity management when a network operator offers its services to a 3rd party application provider. In [20] a toolkit for facilitating the development of privacy-sensitive ubiquitous computing applications is presented. It identifies requirements that must be satisfied by both end-users and application developers. Precision [15] is a system for privacy enhanced context-aware information fusion in ubiquitous computing environments. It introduces the concept of privon that consists of a session id, privacy settings, services and a data window. Data in a privon can exist in one of three classes: transparent, protected, or private. Depending on the privacy settings, the data window can be updated incorporating data elements from protected or private data.

5. ACCESS CONTROL AND PRIVACY ENHANCEMENT IN XEW

Given the security risks enumerated in section 2 and the privacy threats in section 3, few CIS are equipped of a security service that is part of a project who meets a predetermined security and privacy policy. Rather, the responses to a security attack are cobbled together at the sandstone of the dysfunctions in the system. Indeed, people collect explanations for such events after they've occurred, making them seem less surprising and more predictable than they really are. This hindsight causes people to underestimate risks with complex systems as CI platforms [21].

To contribute in a solution of the mentioned weaknesses, we present an approach of Access Control that spans the entire lifecycle of CI platform activity. Our approach of Access Control is focused both on the information that must be bring to decision-makers and the privacy of individuals whose data was used to extract this information.

5.1. Description of Xplor Every Where

XEW is a web service of the CIS TETRALOGIE1 [22][23] that performs global strategic analysis on aggregate or factual coming from online bibliographic databases, CD-Rom, Internet or any other computerized source. Through descriptive and statistics exploratory methods of data, XEW display, in a very short time, new strategic knowledge such as: the profile of the actors, their reputation, their relationships, their sites of action, their mobility, emerging issues and concepts, terminology, promising fields etc.

5.1.1. Activity Life Cycle

As shown in figure 2, strategic analysis and watching are the basic methodology of the process of Information Fusion in XEW.

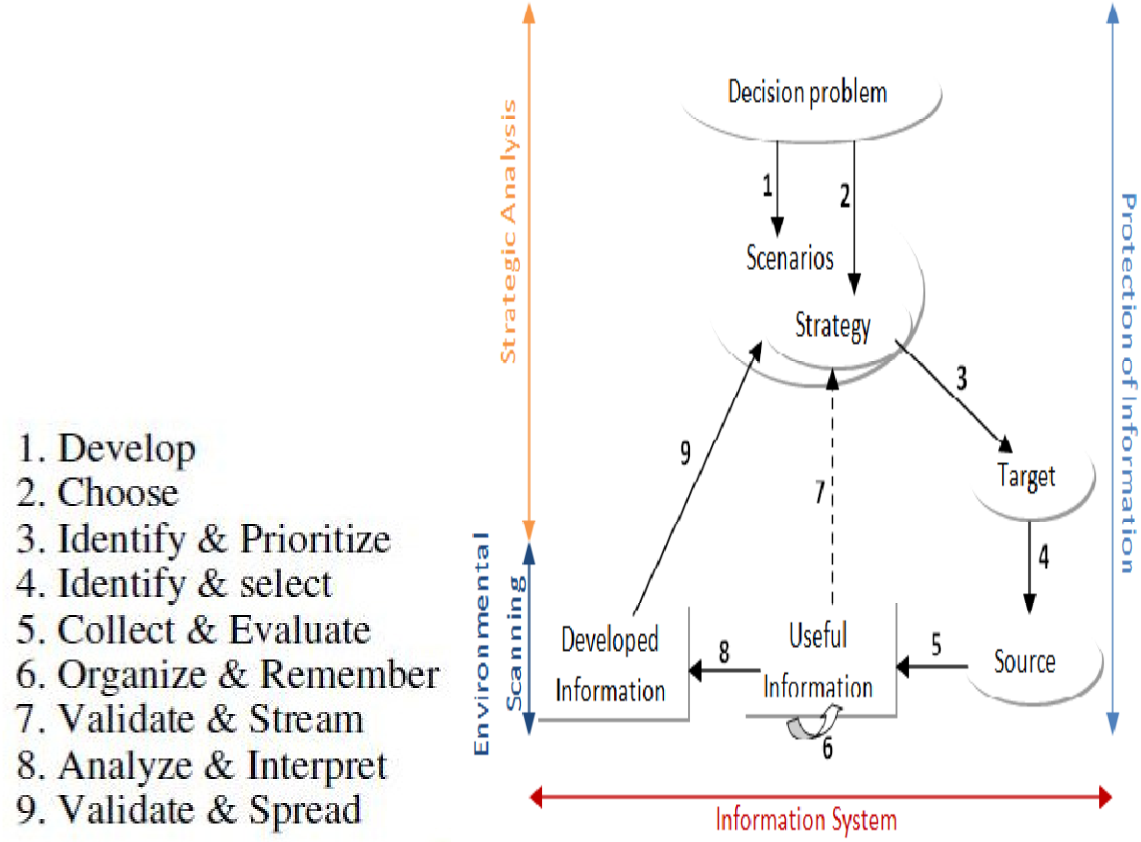


Figure 2. Xplor Every Where Intelligence Process

5.1.2. The platform architecture

The architecture of our platform consists in four main services as shown in figure 3:

- Monitoring Service: A request is generated on the data source (scientific database,Patents database, RSS, Blogs, etc.) to collect data depending on the client's needs. Collected data will form the Corpus.

- Homogenization and structuring Service: Diversity of data source leads to heterogeneous data (format, language …) that must be restructured. At the end, this service defines a unified view of documents in the corpus.

- Reporting service: Reporting is the service responsible for presenting the analysis results to the decision-makers according to the push strategy (IPhone Service, SMS Service, and E-mail Service) or pull strategy (Web Site Service).

- Security Administration Service: Orthogonal to all three mentioned services, it controls data access and ensures the preservation of privacy during the treatments. The section 4.2 explains in detail this service.

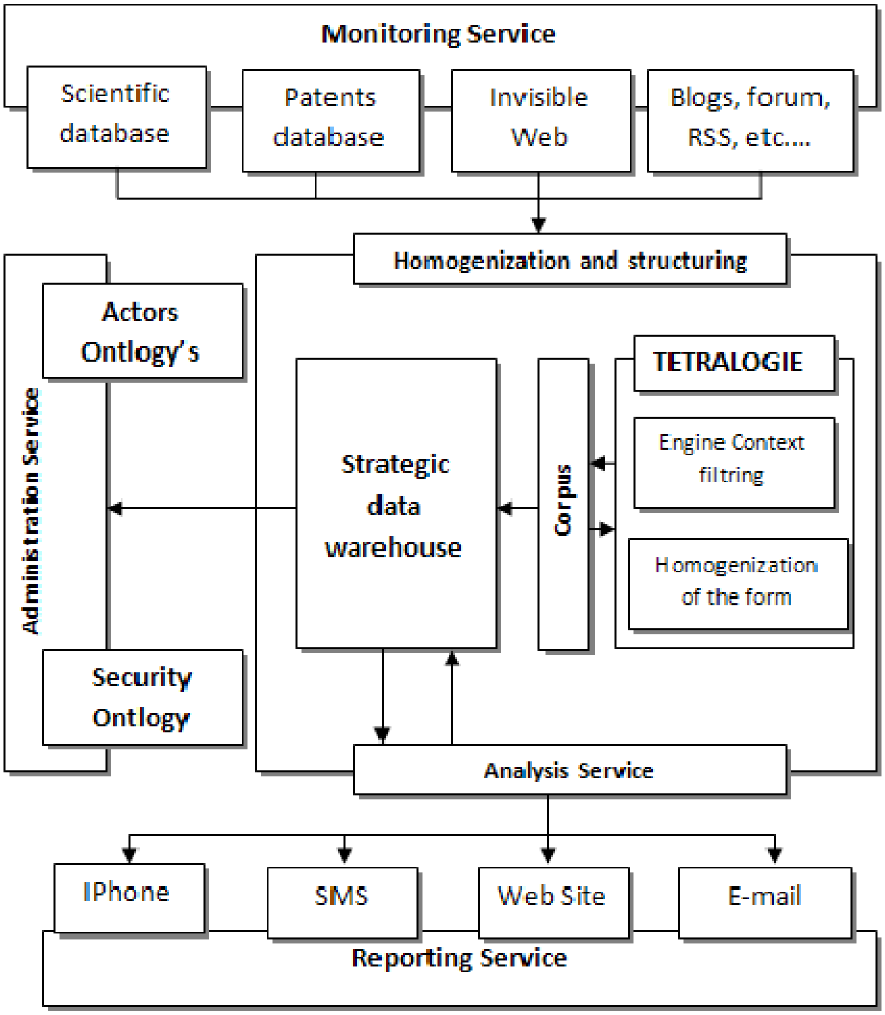


Figure 3. Xplore Every Where Architecture

5.2. Privacy Preservation in Xplor Every Where

People must be aware of information collection and their rights regarding that collection before we can use them. Basing on fair information practices in the electronic marketplace [16], we provide good practices as shown in figure 4. These good practices include:

- Providing a clear and visible privacy protection policy that is writing in the language of all collected data. This policy explains the activities and is presented as a checklist rather than a flat text in order to be closely understandable.

- The policy is available prior to or at the time that individually identifiable information is collected or requested.

- The policy states clearly: what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information.

- Data security and access: We take appropriate measures to enssure data reliability and take reasonable precautions to protect it from loss, misuse or alteration. We establish appropriate mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information may be corrected.

- This privacy policy is inefficient if a good access control policy is not established with adequate mechanisms. In what follows, we explain our access control policy in XEW.

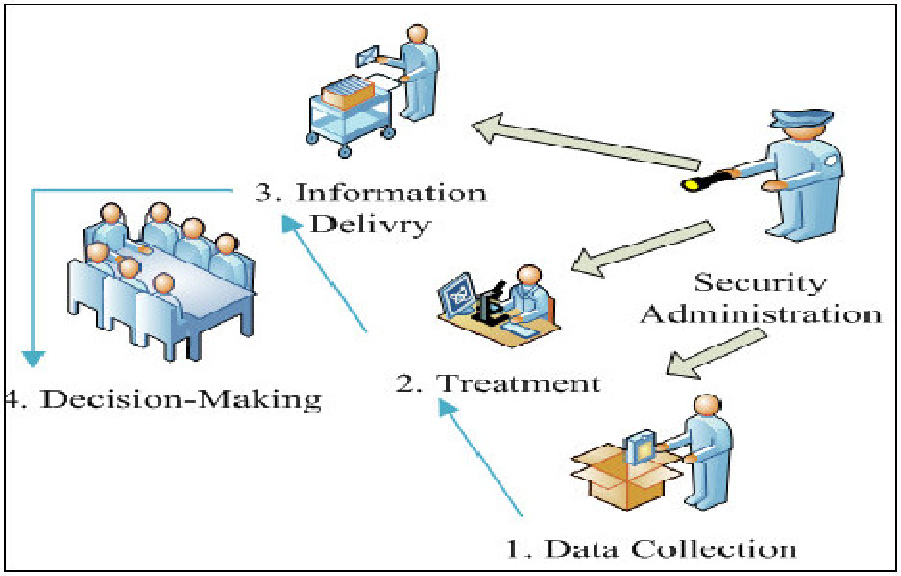


Figure 4. Access and privacy Control in Xplor Every Where

5.3. Access Control Policy in XEW

The approach of Access Control in XEW is based on RBAC (Role Based Access Control), the well known access control standard [24].

In RBAC environments, first, a system administrator defines a set of roles and for each role, he associates a set of access privileges to specific computer resources. Each user will access to the system only based on the role he plays. When the user interacts with the computer system, the user is logged in and can, therefore, specify which subset of roles he is assuming at any given time. However, the user may not be logged in when the computer system executes a usercreated automated task. The RBAC environment allows the user to assume a subset of the assigned roles at a given time.

Main entities in RBAC are Users, Roles, Permissions and Sessions. We define:

- U = Set of all users, {u1,u2,…,uk}. A user can be a humane actor as it can be an automatic process.
- R = Set of roles, {r1,r2,…,rl}.
- P = Set of permissions, {p1,p2,…,pm}.
- WS = {ws1, ws2, …wsn}, a set of sessions.

The security administrator makes associations between these different entities at the administration time of the system. These associations don't be effective until activation of roles by users involved in a proceeding workflow instance.

- UA $\subseteq$ U × R: a many-to-many user-to-role assignment relation.
- PA $\subsetneq$ P × R: a many-to-many permission-to-role assignment relation.

5.3.1. Process Modeling

For a complete visibility and a better control of information flow, we represent all the business processes of XEW in a workflow (a set of tasks related by the dependency and inheritance). Indeed, we are interested only in modeling task access control in terms of permissions. Each execution of the workflow by a system user is a workflow instance ws, which corresponds to a session in the RBAC model. We define it as a quadruple ws = (W, u, state, id) where:

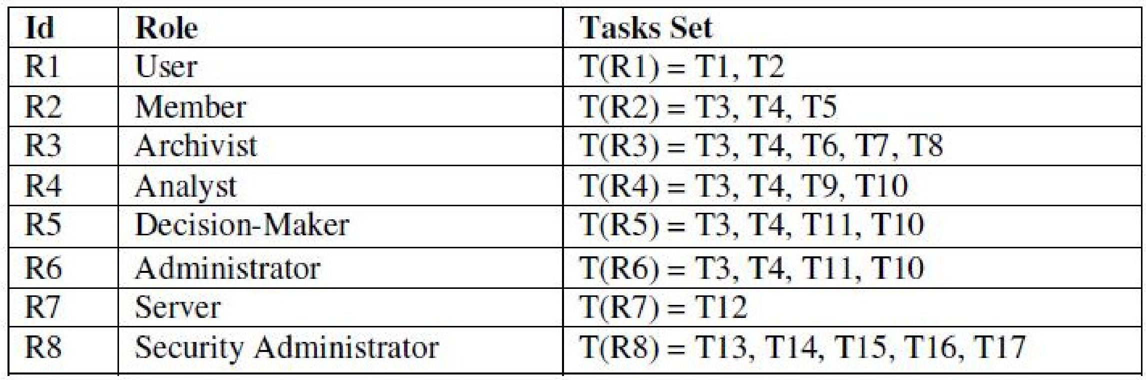
- W is the workflow instanced by ws.
- u : The user who initiated ws
- State: state of was that can be Initiated (running), Suspended, Completed, etc..
- id : ws's identifier

Indeed, we are interested only in modeling access control at the task in terms of permissions regardless of the rules (for example, Precedence) related to the deployed workflow model

5.3.2. Identification of different Roles and their associated tasks

There are eight roles in XEW. Security administration is so simplified since the number of roles in any organization is usually much smaller than the number of users in that organization [25]. By granting permissions to roles played by users rather than to users themselves, users with similar functions can be grouped under the same role. Likewise, the modification of access controls configuration is not required each time someone joins or leaves an organization.

Table 1. Roles and associated tasks



Id	Role	Tasks Set
R1	User	T(R1) = T1, T2
R2	Member	T(R2) = T3, T4, T5
R3	Archivist	T(R3) = T3, T4, T6, T7, T8
R4	Analyst	T(R4) = T3, T4, T9, T10
R5	Decision-Maker	T(R5) = T3, T4, T11, T10
R6	Administrator	T(R6) = T3, T4, T11, T10
R7	Server	T(R7) = T12
R8	Security Administrator	T(R8) = T13, T14, T15, T16, T17

- T1: Consulting the application Home
- T2: Request a registration
- T3: Consult the analysis list
- T4: Perform a Search
- T5 : Request an analysis
- T6: Add a corpus
- T7: Consult a corpus
- T8 : Delete a corpus
- T9: Perform an analysis
- T10: Delete an analysis
- T11: Validate an analysis
- T12: Update the BDD
- T13: Add a role
- T14: Delete a role
- T15: User Authentication
- T16: Grant permissions
- T17: Validate the credibility of data source

5.3.3. Role Hierarchies and Role delegation

The role set can be more optimized if a hierarchy relation is maintained between the roles. The notion of role hierarchy allows senior roles to inherit the permissions of the corresponding junior roles. Delegation is the fitness that a user (say, Alice) delegates to another user (say, Beth) the right to perform a task for a particular workflow case [26]. This is necessary to continue the activity even if a given user is unavailable Role hierarchies and delegation relations are done under the principle of Separation of Duty (SoD) and Least Priviledge (LP) [27].

5.3.4. Conflicting entities

The access control policy limits user's permission to avoid information leakage. But this mechanism alone is not sufficient to achieve the goal: conflicting entities, if they are joined together can overcome the access control policy and compromise the security. Four types of conflict are possible in XEW:

- Conflicting permissions: They allow a user to have more rights than necessary. This conflict must be checked when a user an inherits (as well as if he delegates) privileges to user b.
- Conflicting roles: if they are able to conspire
- Conflicting users: if they will have together sufficient power to collude, and are likely to do so. In practice, this may be family members.
- Conflicting tasks: if they are associated with conflicting users or conflicting roles.

5.3.5. Identification of objects to be protected

A role is nothing but a set of permissions. The permissions granted to a role are operations on objects. On the XEW the objects to be protected are:

- The web portal platform.
- Internal documents: dashboards, management document, internal procedure manuals, minutes of meetings and visits...
- External documents: letters and e-mails, resumes, etc.
- Softwares and applications: meta-search engine, Web Crowlers, data mining tools, etc.
- The corpus.

5.3.6. Security Infrastructure

- Cryptographic tools: To encrypt sensitive data exchange, particularly when delivring information to decision-makers.
- Historical access repository: To trace all activities. At any time, for a given user, this reference provides information on the activated roles, performed tasks and the time required for execution.
- Worklist management: For a given session (each time a user selects a role to perform a given task), a corresponding worklist is generated in accordance with security policy and on the basis of historical repository. It explains all possible actions for the given

user and allows the security administrator to grant or deny access to each step.

6. CONCLUSION

The need for CI has never been greater, as the gap between the amount of information available and our ability to analyze and understand it is widening. The magnitude of data to be analyzed requires the watchers spend all their time in information fusion, forgetting sometimes to properly secure their systems. Unfortunately, the damage resulting from security weaknesses are more expensive than income of opportunity. We have presented an access control model that each task in a CIS is performed only by authorized users.

On the other hand, the fact that people continue to provide information about them represents the commercial capital in a CIS. Therefore, preserving privacy should not be perceived as a constraint (to comply with the law), but rather, it is all in our interest. For this reason, the security model that we present in this paper provides guarantees (in term of privacy preservation) to individuals to continue to provide information about them. So a privacy preservation policy is integrated through the lifecycle of the access control model to reduce security threats during competitive intelligence activity.

REFERENCES

[1] R. G. Vedder, M. T. Vanecek, C. S. Guynes, and J. J. Cappel, "CEO and CIO Perspectives on Competitive Intelligence", Communications of the ACM, Vol. 42, N°8, 1999, (pp 108-116).

[2] P. Guarda, N. Zannone, "Towards the development of privacy-aware systems", Information and Software Technology, Vol. 51, N°2, 2009, (pp 337-350).

[3] J. Hulstijn, J. Gordijn, "Risk analysis for inter-organizational controls", In Proceedings of the 12th International Conference on Enterprise Information Systems (ICEIS 2010), 2010, (pp314-320).

[4] Club de la Sécurité de l'Information Français, "Menaces informatiques et pratiques de sécurité en France", 2008.

[5] J. Bleiholder, F. Naumann, "Data Fusion", ACM Computing Surveys, Vol. 41, N° 1, 2008, (pp 1-41).

[6] I. Corona, G. Giacinto, C. Mazzariello, F. Roli, C. Sansone, "Information fusion for computer security: State of the art and open issues", Information Fusion, Vol. 10, N°4, 2009, (pp274-284).

[7] E. B. Talbot, D. Frincke, M. Bishop, "Demythifying Cybersecurity", IEEE Security & Privacy, Vol. 8, N° 3, 2010 (pp 56-59).

[8] J-P Bichard, "De la veille stratégique à la sécurité de l'information, Décision Informatique", N° 625, Mars 2005, (pp 8-9).

[9] J. Madhavan, D. Ko, Ł. Kot, "Google's DeepWeb Crawl", Proceedings of the VLDB Endowment (PVLDB' 08), Vol. 1, N° 2, 2008, (pp 1241-1252).

[10] I. P. Cook, S. L. Pfleeger, "Security Decision Support Challenges in Data Collection and Use", IEEE Security & Privacy, Vol 8, N° 3, 2010, (pp 28-35).

[11] B. M. Bowen, M. Ben Salem, S. Hershkop, A. D. Keromytis, S. J. Stolfo, "Designing Host and Network Sensors to Mitigate the Insider Threat", IEEE Security & Privacy, Vol 7, N° 3, 2009, (pp 28-35).

[12] M. Ben Salem, S. Hershkop, S. J. Stolfo, "A Survey of Insider Attack Detection Research", Advances in Information Security, Vol. 39, 2008, (pp 69-90).

[13] A. Shabtal, Y. Fledel, Y. Elovici, "Securing Android-Powered Mobile Devices Using SELinux", IEEE Security & Privacy, Vol 8, N° 3, 2010, (pp 36-44).

[14] R. Di Pietro, L. V. Mancini, "Security and Privacy Issues of Handheld and Wearable Wireless Devices", Communications of the ACM September, Vol. 46, N° 9, 2003, (pp 75-79).

[15] G. Pallapa, N. Roy, S. Das, "Precision: Privacy Enhanced Context-Aware Information Fusion in Ubiquitous Healthcare", Proceedings of the 1st International Workshop on Software Engineering for

Pervasive Computing Applications, Systems, and Environments (SEPCASE'07), 2007.

[16] R. Pitofsky, S. F. Anthony, M. W. Thompson, O. Swindle, T. B. Leary, "Privacy online: Fair Information Practices in the Electronic Marketplace", A Report to Congress, Federal Trade Commission, 2002, http://www.ftc.gov/reports/privacy2000/privacy2000.pdf, Accessed on July 01, 2010.

[17] G. Ghinita, P. Kalnis, Y Tao, "Anonymous Publication of Sensitive Transactional Data", IEEE Transactions on Knowledge And Data Engineering, Vol 22, N°6, 2010

[18] G Iachello, J. Hong, "End-User Privacy in Human-Computer Interaction", Foundations and Trends in Human-Computer Interaction, Vol. 1, N°1, 2007, (pp1-137).

[19] O. Jorns, G. Quirchmayr, O. Jung, "A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services", Proceedings of the fifth Australasian symposium on ACSW frontiers, 2007, (pp133 – 142).

[20] J. I. Hong, J. A. Landay, "An Architecture for Privacy-Sensitive Ubiquitous Computing", Proceedings of the 2nd international conference on Mobile systems, applications, and services, 2004, (pp 177 – 189).

[21] K. J. Hole, L-H. Netland, "Toward Risk Assessment of Large-Impact and Rare Events", IEEE Security & Privacy, Vol. 8, N° 3, 2010, (pp 21-27).

[22] B. Dousset, Integration of interactive konwledge discovry for envirnmental scanning. Phd. Rapport , University Paul Sabatier, Toulouse, (2003).

[23] A. El Haddadi, B. Dousset and I. Berrada, “Xplor EveryWhere – A tool for competitive intelligence on the web and mobile”, VSST 2010, Toulouse, (2010).

[24] ANSI. American national standard for information technology – Role based access control. ANSI INCITS 359-2004, February 2004

[25] D. F.Ferraiolo, D. R. Kuhn, and R. Chandramouli, "Role-Based Access Control, 2nd ed., Norwood, MA: Artech House, 2007

[26] J. Wainer, A. Kumar, P. Barthelmess, "DW-RBAC: A formal security model of delegation and revocation in workflow systems", Information Systems, Information Systems, Vol.32, N° 3, 2007 (pp365-3384).

[27] H. El Bakkali, H. Hatim, "RB-WAC: New approach for access control in workflows", The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA’09), May 10-13, 2009 (pp 637-640).