A NEW ACCESS CONTROL MODEL BASED ON THE CHINESE WALL SECURITY POLICY MODEL

M Loock and J H P Eloff

Information and Computer Security Architectures Research Group,

Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa

loockm@unisa.ac.za, eloff@cs.up.ac.za

ABSTRACT

Access control policies and models guide the successful implementation of well-defined access control requirements, which are used for the protection of information or data objects in an information system environment.

Whenever these objects are used in a data mining environment, a change in the access control requirements is needed. During a data mining activity, the data miner may expose unexpected results or trends. All companies involved in data mining activities should be aware of these potential access control problems. Effective security policies can, however, help resolve these problems. Brewer and Nash (1989) first defined the Chinese Wall Security Policy model (CWSP model). This model provides access control for the commercial environment based on *conflict of interest classes*. Shortly after the introduction of the model, Lin (1989) reported an error and presented a modified version of the model called the Aggressive Chinese Wall Security Policy model (ACWSP model). This model introduced the concept of an overlap between conflict of interest classes. When the access control requirements needed for a data mining environment were investigated, it became evident that these two models did not fully comply with the requirements.

The purpose of this article is to discuss a new access control model, based on the Chinese Wall Security Policy model, for a data mining environment. This new model will cover the access control requirements not met in the existing models.

With this new access control model, data miners will be able to work on different company information or data objects without causing access control problems such as information leakage following exposure to unexpected results or trends. All companies involved in data mining activities will be able to control their level of exposure among competitive peer companies if they use the proposed access control model. The new model is dynamic in that it can cope with a rapidly changing business environment.

KEYWORDS

Information security, Chinese Wall Security Policy model, Aggressive Chinese Wall Security Policy model, security policy model, data mining, access control

1 INTRODUCTION

In general, access control policies and models guide the successful implementation of well-defined access control requirements, which are used for the protection of real-world information or data objects in an information system environment. When data mining is done on such protected real-

world information or data objects, the implementation of the current access control policies and models may not be sufficient to protect the results of such data mining activities.

Data mining is a well-defined and structured activity through which derived information is obtained from large masses of basic or core data. Because it uncovers meaningful patterns and rules, data mining provides an organisation with useful intelligence (Berry & Linoff, 1997). This derived information or intelligence is essential for organisations to be competitive. The information can be used in areas such as business management, market analysis and science exploration. The data mining process does not cease the moment the derived information becomes available. The derived information, in whatever format it is presented, for example types of graphs or text, may create an information security risk problem by revealing new and unexpected information. Access control policies and models, for example security policy models, should be able to improve the security of such unexpected information.

Security policy research concentrates on military security policies and commercial security policies. The Bell and LaPadula security model (1973; 1975) is a formalization of the military security policy and was followed by the Biba security model (Biba, 1977). The Clark and Wilson security model (Clark & Wilson, 1987) highlighted the importance of commercial security policy models and two years later Brewer and Nash (1989) defined the Chinese Wall Security Policy (CWSP) model. In the same year, Lin (1989) defined the Aggressive Chinese Wall Security Policy (ACWSP) model for a commercial environment. All of these models were designed to operate in a well-defined environment ranging from a strict military environment to a commercial environment. Unfortunately, they did not address access control problems related to derived information such as in a data mining environment.

This article suggests the addition of new definitions for an existing access control model, the CWSP model. The new access control model will be functional in a commercial environment where data mining activities take place, and it will help solve the data mining information leakage problem. The next section of the article describes the access control problem by means of a banking example. Subsequent sections indicate why the CWSP model does not meet the access control requirements of DM Bank and explain a new access control model for a data mining environment.

2 ILLUMINATION OF THE PROBLEM BY MEANS OF AN EXAMPLE

The following example illustrates the access control problem that exists in a commercial environment where data-mining activities take place.

DM Bank (Figure 1) is a financial institution with hundreds of clients in the business sector. DM Bank also has a section that does data mining on all DM Bank databases for prediction, marketing and risk management purposes (Berry & Linoff, 1997). Among the techniques used is a ‘decision tree’ technique (Berry & Linoff, 1997; Shi, 2000). Airline Companies A, B and C; Petroleum Companies D and E; and Food Companies F, G, H and J are all clients of DM Bank.

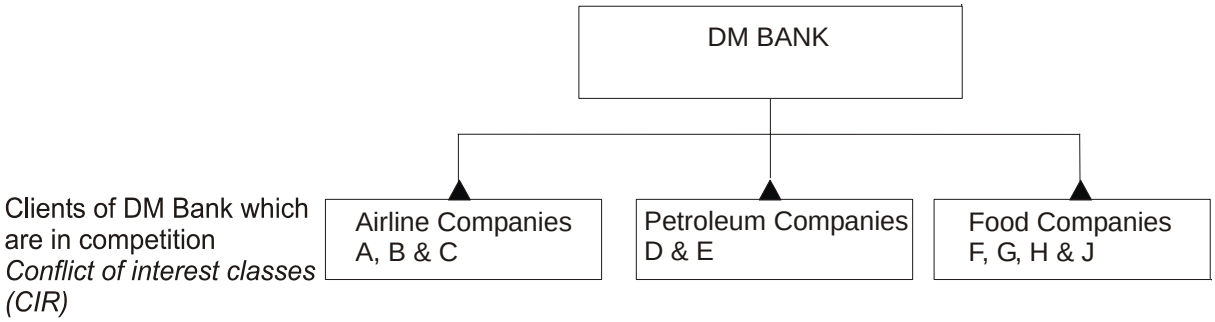

Figure 1: DM Bank

Let us assume that Airline Company A bought shares in Petroleum Company D for $10 a share. From its data mining exercise, DM Bank detects a negative growth in Petroleum Company D's cash flow. Petroleum Company D is exposed to an unwanted information security risk problem through possible information leakage – DM Bank could 'leak', by accident, this sensitive information to Airline Company A. The information leakage could damage Petroleum Company D if the parties involved (DM Bank and Petroleum Company D) do not enter into mutual confidentiality agreements.

DM Bank should reconsider access control as a means of solving the information leakage problem. Different data mining issues should also be considered by DB Bank, for example, 'What is DM Bank allowed to do after the results of the data mining process are revealed?' and 'Who can gain access to the mined information?' To manage and control responses to these questions, DM Bank needs a security policy that can be applied to an environment that consists of already mined information. This implies that a security policy should be implemented using security models, for instance file access control models that can deal with the identified threat.

The current CWSP model, as well as the ACWSP model, are two access control models that could be considered in this regard.

3 WHY THE CWSP MODEL DOES NOT MEET THE ACCESS CONTROL REQUIREMENTS OF DM BANK

The CWSP model involves actors (data miners) and objects (information or data objects). It contains a set of rules aimed at preventing people from accessing information or data objects on the wrong side of a wall. This model defines the access right to information or data objects to which the actor (data miner) already holds title. All corporate information, DM Bank's information, is stored in a hierarchy as shown in Figure 2.

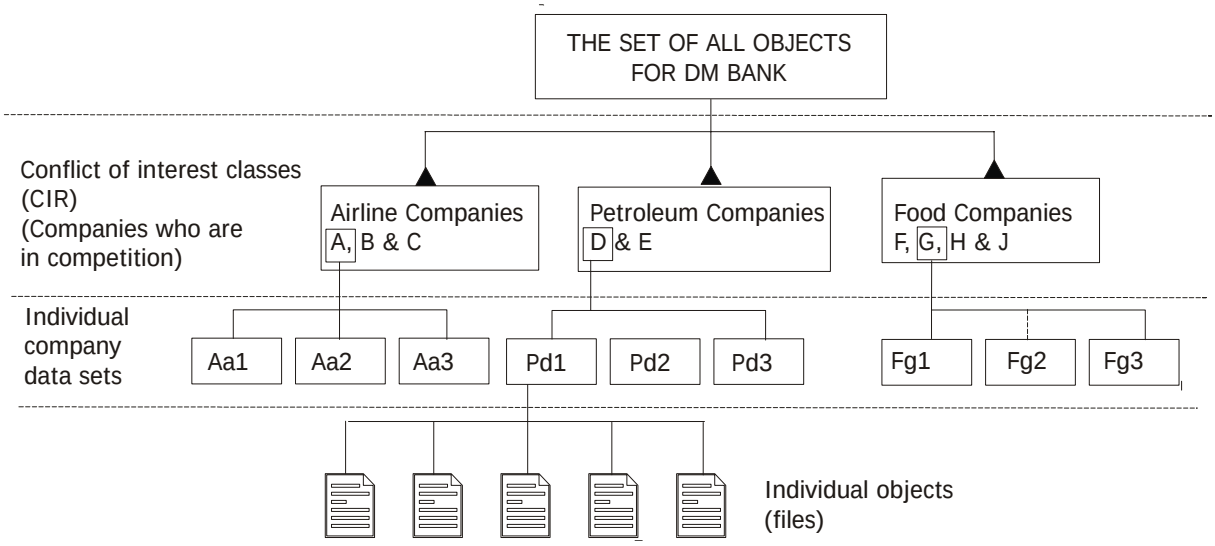

Figure 2: DM Bank and the Chinese Wall Security Policy model

Three levels of significance pertain: At the lowest level, individual objects containing specific data items, each concerning a specific company, are considered.

At the intermediate level, all objects concerning the same company are grouped together and referred to as 'company data sets'.

At the highest level, all company data sets whose companies are in competition (conflict) are grouped together. They are referred to as 'conflict of interest classes' (CIR).

Each object is associated with the name of the data set of the company to which it belongs and the name of the conflict of interest class to which that company belongs. For example, the conflict of interest class names could be the business sector headings found in stock exchange listings (Petroleum Companies, Airline Companies and Food Companies), while the individual companies could be the names of companies listed under those headings.

If the data mining environment of DM Bank contains information on Airline Company A, Petroleum Company D and Food Company G –

1. All objects would belong to one of three company data sets – company data set Airline Company A or company data set Petroleum Company D or company data set Food Company G, and
2. There would be three conflict of interest classes, one for Airline Companies (containing Airline Companies A, B and C's data sets), one for Petroleum Companies (containing Petroleum Companies D and E's data sets), and one for Food Companies (containing Food Companies F, G, H and J's data sets).

The basis of the Chinese Wall Security Policy model is that people are allowed access only to information that is not in conflict with any other information that they already possess. When considering the DM Bank scenario, and if data mining activities have already been carried out, a new data miner may be assigned to whatever data sets DM Bank chooses. As far as the CWSP model is concerned, a new data miner does not possess any information at this stage, and therefore no conflict of interest can exist. However, such a conflict may arise later on.

Let us assume a data miner accesses Airline Company A's data sets first; at this stage, he/she possesses information concerning Airline Company A's data sets. Since Airline Company B is in

conflict/competition with Airline Company A, the data miner will therefore not be granted access to Airline Company B's data sets. However, he/she will be permitted to request access to Petroleum Company D's data sets because the data sets of these two companies belong to different conflict of interest classes. According to the CWSP model, this is permissible because the Airline Companies and the Petroleum Companies are not in competition and therefore are in different conflict of interest classes. However, when a higher level, called the data mined level, is being worked on, as in the DM Bank example, this should not be allowed. Knowing information pertaining to Petroleum Company D (namely the negative change in Petroleum Company D's cash flow situation mentioned earlier) and making it known to Airline Company A (which has shares in Petroleum Company D) puts Petroleum Company D at risk. It is therefore inappropriate for DM Bank to use the CWSP model because the information leakage problem will not be solved.

A new access control model will be suggested. This model will obviate the abovementioned information leakage problem and will also address the following important issues.

- CIR classes can and may overlap – this is to accommodate the conflict of interest between, for example, Airline Company A and Petroleum Company D. Lin (1989) dealt with the problem pertaining to the CIR classes that can and may overlap in the ACWSP model.
- The severity of the conflict/competition between two companies should be definable. A conflict of interest may exist between Airline Company A and Food Company G, but it may be so small that it needs no extra mentioning and should not inhibit access capabilities.
- A Security Policy model should also be dynamic. If Airline Company A sells all its shares in Petroleum Company D, the companies are no longer in conflict and should be treated accordingly.

Lin (1989) dealt with the *CIR classes that can and may overlap* problem in the ACWSP model. An overview of the ACWSP model and an example illustrating this problem are given in paragraph 3.1.

3.1 The Aggressive Chinese Wall Security Policy Model

The CWSP model builds a collection of impassable walls, called 'Chinese walls', around the data sets of competing companies. No data that are in conflict can be stored on the same side of the Chinese walls. According to Lin (1989; 2003), the Brewer-Nash model was based, among other factors, on the *incorrect assumption* that corporate data can be grouped into separate and disjointed conflict of interest classes (CIR classes). For example, an incorrect assumption would be that all Airline Companies could be grouped into one, and only one, conflict of interest class. CIR classes are seldom disjointed – they do overlap.

Lin suggested a modified model called the Aggressive Chinese Wall Security Policy model (ACWSP model). This model is based on the development of a methodology called 'Granular Analysis and Computing' (Lin, 2003).

To illustrate the error in the CWSP model's assumption that the set of all objects of DM Bank could be partitioned into mutually disjointed CIR classes, let us revisit the example in Figure 1. Airline Company A is in the conflict of interest class for all Airline Companies. Petroleum Company D is in the conflict of interest class for all Petroleum Companies. This means Airline Company A and Petroleum Company D have no conflicting interests, but this is not true because of the *shares* between the two companies. This also means that Airline Company B and Petroleum Company D have no conflicting interest, which is true in this case. These two CIR classes are distinct but they overlap, as depicted in Figure 3.

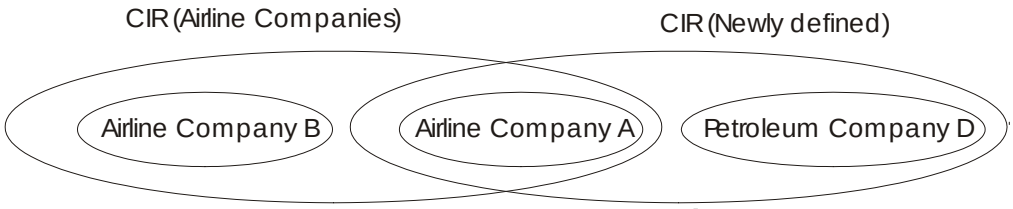

Figure 3: CIR classes are distinct but they overlap

The ACWSP model puts DM Bank in the position where friends and enemies can be defined by means of a discretionary access control (DAC) approach (Carroll, 1996). The model implies that Airline Company A and Petroleum Company D can be defined as companies in the same CIR class. Furthermore, it also implies that the ACWSP model will solve the problem of the mutually disjointed CIR classes that existed in the DM Bank environment when the standard CWSP model was used.

If DM Bank uses the ACWSP model, the 'CIR classes can and may overlap' problem is solved, but the following important issues remain unresolved.

- The *severity* of the *conflict* between two companies should be definable. A *conflict of interest* may exist between Airline Company A and Food Company G, but it may be so small that it needs no extra mention and should not inhibit access control.
- Another requirement of a Security Policy model is that it should be *dynamic*. If Airline Company A sells all its shares in Petroleum Company D, the companies are no longer in conflict and should be treated as such.

The Security Policy model used when doing data mining in a commercial environment should be *dynamic* to accommodate an unpredictable environment that can change rapidly.

4 A NEW ACCESS CONTROL MODEL FOR A DATA MINING ENVIRONMENT

By adding to the CWSP model's definition, the environment that consists of already mined information could be covered as well.

This article suggests three new definitions: Two definitions to be added to the current CWSP model and one that changes the original 'conflict of interest class' definition of the CWSP model. The first definition for discussion is the 'conflict of interest class' definition that will be changed slightly to a 'conflict of interest area' definition.

4.1 Definition 1: Conflict of interest area

A set of companies (all DM Bank's clients) exists where each company has a 'conflict of interest area' around it. This 'conflict of interest area' is also referred to as a sphere of conflict with radius r. Let us consider the following example. ABC Petrol Company has a 'conflict of interest area' defined around it involving companies like P+P Petrol Company and Green Petrol Company. (Figure 4)

Other companies that can also be in this 'conflict of interest area' around ABC Petrol Company are Pick&Save Food Company and HighFly Airline Company. The last two companies are in this 'conflict of interest area' because ABC Petrol Company has shares in QuickPay Food Company, which is in competition with Pick&Save Food Company, and ABC Petrol Company also has shares in FlySave Airline Company, which is in competition with HighFly Airline Company.

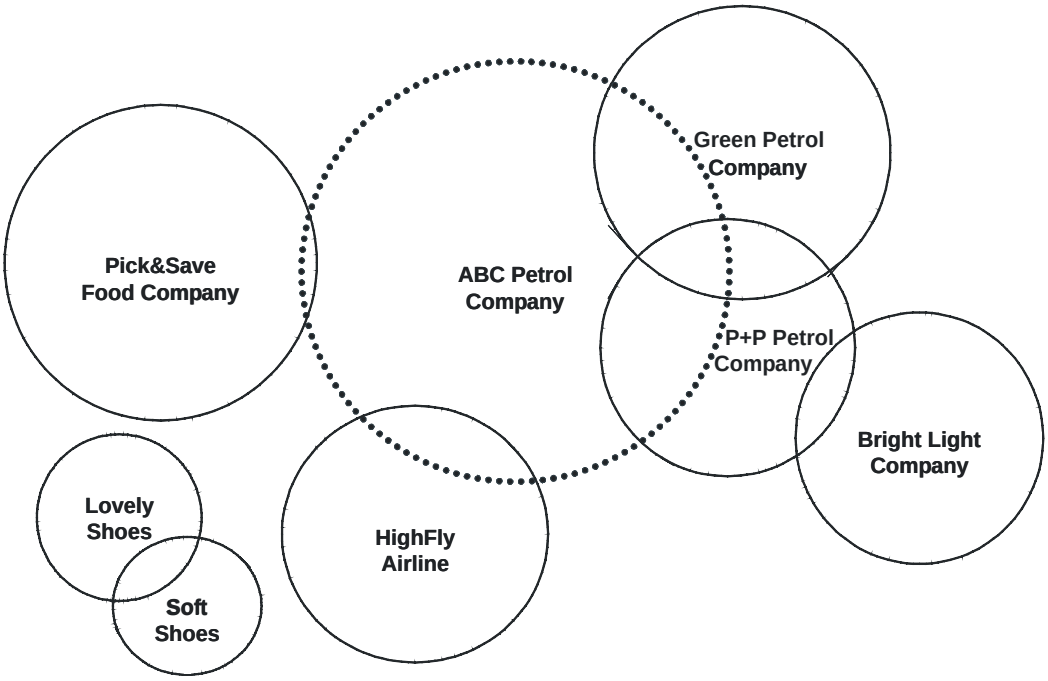

Figure 4: Conflict of interest areas

The second definition is called a 'distance' definition; it defines the severity of conflict between a primary company and any of its conflicting/competing companies at any given time.

4.2 Definition 2: Distance

The distance definition is formulated for a primary company (e.g. ABC Petrol Company) within a set of companies. This set of companies is a combination of all the companies that are in conflict with the primary company. The distance definition reflects the severity of the conflict between the primary company and any one of its conflicting companies, as seen by the primary company, which is ABC Petrol Company in this example. The value of the distance definition will always be positive. A distance = 0 implies that the model is working with the same company, for example the distance between ABC Petrol Company and itself = 0. A distance = ∞ implies an infinite distance, which means no conflict of interest exists between the primary company and a specific company, for example ABC Petrol Company and Lovely Shoes Company.

Drawing a circle around ABC Petrol Company and placing all the companies that are in conflict with ABC Petrol Company at a predefined distance from ABC Petrol Company will result in a 'conflict of interest area'. The predefined distance between ABC Petrol Company and, for example, P&P Petrol Company is the radius that defines the severity of the conflict between these two companies as seen by ABC Petrol Company. This radius can, for example, be defined as 1 for all Petrol Companies, radius = 2 for HighFly Airlines and radius = 3 for Pick&Save Food. This is graphically illustrated in Figure 5.

To be able to answer the question whether a conflict of interest exists between any two companies at a given time, the 'Path' definition is used.

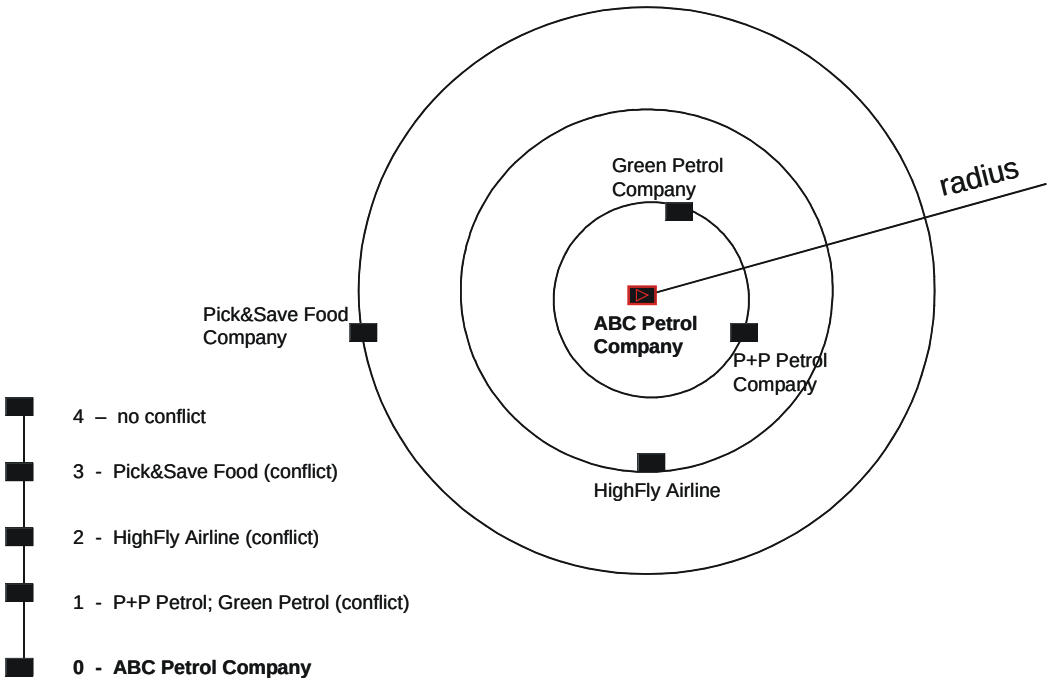

Figure 5: Distance = radius – defines severity of conflict between companies

4.3 Definition 3: Path

The distance definition enables the definition of a path. The existence of a path implies a conflict of interest between the two companies at both ends of the path. The distance of the path is a positive number. When no path between two companies exists, the distance = ∞. For example, as depicted in Figure 6, if data miner #01 is working with ABC Petrol Company's information, the following two questions are examples of questions that could be asked.

- Question 1: Is this data miner allowed to work on Pick&Save Food Company?
- Question 2: Is this data miner allowed to work on Lovely Shoes Company?

In other words, is the distance between ABC Petrol Company and either of the two companies in question equal to ∞? One possible way to represent the relationships is illustrated in Figure 6.

For Question 1, in Figure 6, the path from ABC Petrol Company to Pick&Save Food Company runs through the ABC Petrol Company area and the Pick&Save Food Company area. The 'distance' or length of this path = 3. This relationship indicates a conflict of interest between ABC Petrol Company and Pick&Save Food Company, and therefore the same data miner cannot work on both companies.

For Question 2, in Figure 6, the data miner who works on ABC Petrol Company will be allowed to work on Lovely Shoes Company because no path exists between these two companies. This results in a path with a value of ∞.

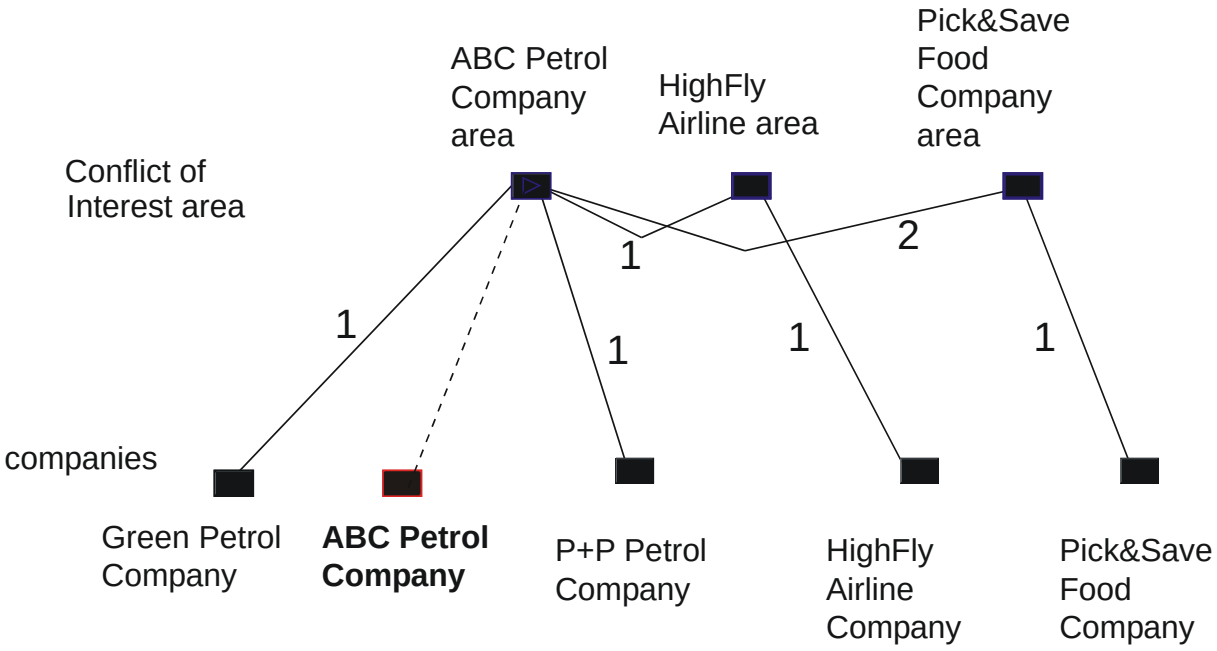

Figure 6: Path between companies

5 CONCLUSION

There is a difference between working with information or data objects in the real world and working with mined information, especially in the definition of security risk areas and the management thereof. When working with mined information, it is impossible to predict whether or not a security risk area will emerge. Procedures should therefore be in place in the event of such a security risk area suddenly materialising so that the risk can be minimised as far as possible.

In this article, an example was discussed to show the limitations of the CWSP model and the ACWSP model when applied to mined information. The article suggests three new definitions that can be added to the CWSP model to sustain a secure state in a data mining environment and thereby minimise risks of access control compromises.

Future work should include the investigation of the transitive relationships between ABC Petrol Company and BrightLight Company through P+P Petrol Company. Each relationship will have to be investigated to determine if it is a conflict relationship or not and if it can be represented on the current structure suggested in Figure 6.

REFERENCES

Bell, D. & LaPadula, L. 1973. *Secure Computer Systems: Mathematical Foundations*, MITRE Corporation, Bedford, MA, Technical Report MTR-2547, Vol. I.

Bell, D. & LaPadula, L. 1975. *Secure Computer System: Unified Exposition and Multics Interpretation*, MITRE Corporation, Bedford, MA, Technical Report MTR-2997 Rev. 1.

Berry, M. J. A. & Linoff, G. 1997. *Data Mining Techniques: For Marketing, Sales, and Customer Support*. John Wiley & Sons, Incorporated.

Biba, K. 1977. Integrity Considerations for Secure Computer Systems, *U.S. Air Forse Electronic Systems Division Technical Report*:76-372.

Brewer, D. F. C. & Nash, M. J. 1989. The Chinese Wall Security Policy, in *IEEE Symposium on Security and Privacy*, Oakland, pp. 206-214.

Carroll, J. M. 1996. *Computer Security*. Third Edition, Newton: Butterworth-Heinemann.

Clark, D. & Wilson, D. 1987. A Comparison of Commercial and Military Security Policies, in *IEEE Symposium on Security and Privacy*, pp. 184-194.

Lin, T. Y. 1989. Chinese Wall Security Policy - An Aggressive Model, in *Fifth Annual Computer Security Applications Conference*, pp. 282-289.

Lin, T. Y. 2003. Chinese Wall Security Policy Models: Information Flows and Confining Trojan Horses, in *Seventeenth Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Estes Park, Colorado, U.S.A.

Shi, Y. 2000. Data mining, In: M. Zeleny, (ed.) *The IEBM Handbook of Information Technology in Business*, pp. 490-495.