

IT security investigation based on vulnerable levels

Tibor Ujbanyi*, Jozsef Katona*, Attila Kovari*

* College of Dunaujvaros/Institute of Computer Engineering, Dunaujv ros, Hungary
ujbanyit@mail.duf.hu, katonaj@mail.duf.hu, kovari@mail.duf.hu

IT security has high priority in a complex, multi user IT system. Security systems and safety measurement are needed to protect data and systems. The maximum protect level is determined by defense against external attacks and connections of users and user groups who access the system. In the article, we examine these user connections, data links and define optimal dispersion of these based on IT security.

GRAPH BASED MODEL OF ACTORS, LINKS AND SHARED OBJECTS

In our simplified model, every user and other system, which have access and modification privileges to shared information (i. e. web or native data client applications) and their groups are called actors. IT resources containing shared information as data elements or complex data structures (computers, servers, data warehouse etc.) are hereinafter referred to as shared objects. Data access links between actors and shared objects (for example computer or telephone networks) represent the ways of information flow. The connection graph can be illustrated by actors and shared objects as nodes and the links as edges. The connection net illustrated by this way can be seen in Figure 1. In this figure, the shared objects are signed with „D1”-„D6”, and the actors with „A1”-„A8” parameters.

In the graph, the A1-A9 actors use and access the D1-D6 shared objects through Ci links in multi-user mode. In IT systems the access privileges can be defined by user or user groups which limit the possible links.

If we consider that each actor is a group of users of a given organization in the graph, these actors can access given shared objects represented by links. The users outside a group are external individuals and all external individuals are potential threat to obtain non-public information belonging to a shared object.

The nets of the graph in Figure 1 can be divided into two separate sets, A and B, which satisfy the criterion that all end of the edges are in A or B disjoint sets. These type of graphs are bipartite graphs.

The complexity of bipartite graph can be easily illustrated by Venn-diagrams. With the help of Venn-diagrams, the structures of the entire graph can be easily demonstrated but this diagram cannot describe the connection density numerically by itself. If the number of connections of a given actor or group of actors are high, the amount of information available by these are probably also high. The probability of external vulnerability is based on the importance of the actor and if the actor can access a lot of information, this probability is higher.

Therefore, it is important to quantify the connection density based on Venn-diagrams.

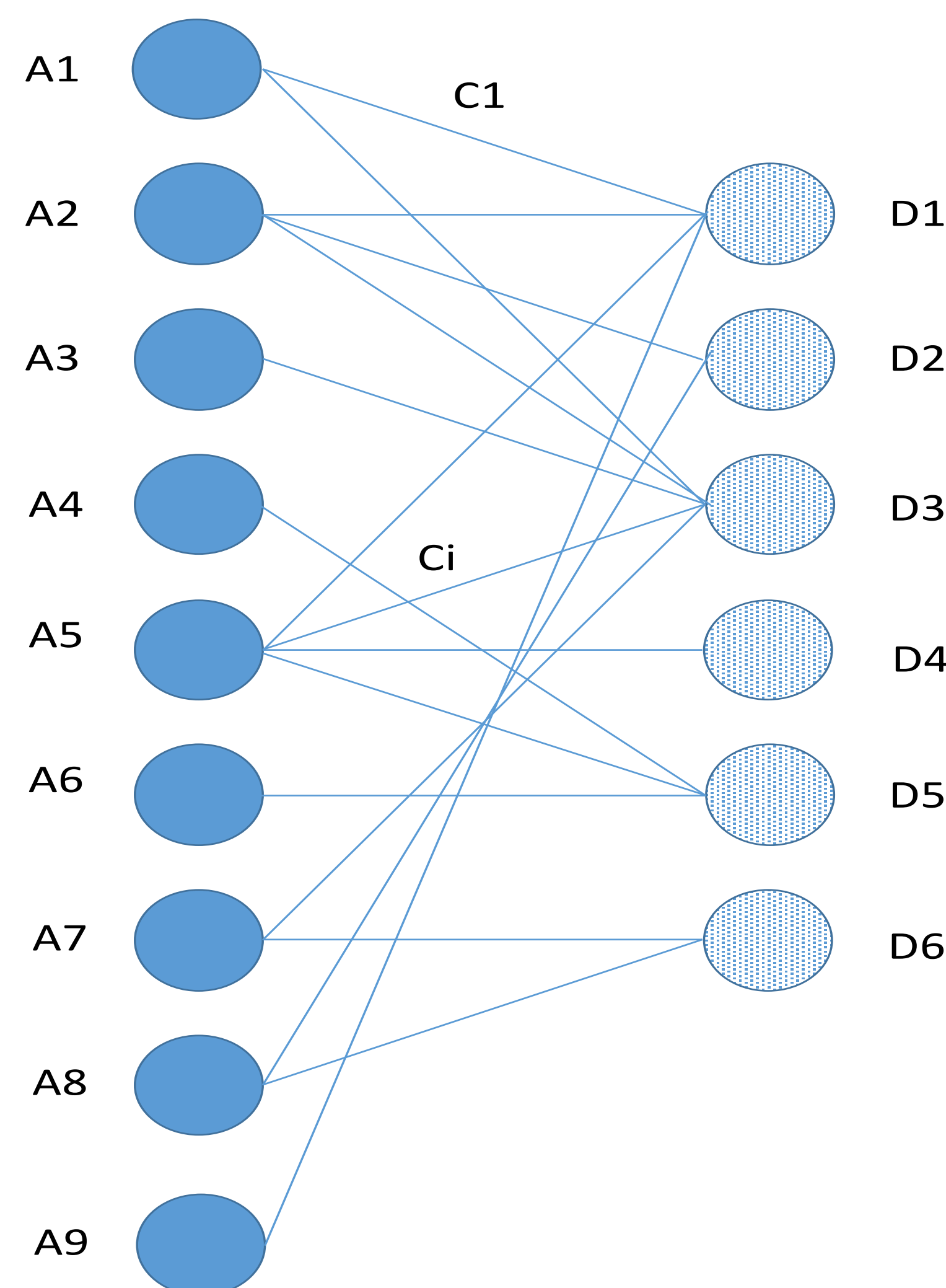


FIGURE 1: GRAPH MODEL OF ACTORS, SHARED OBJECTS

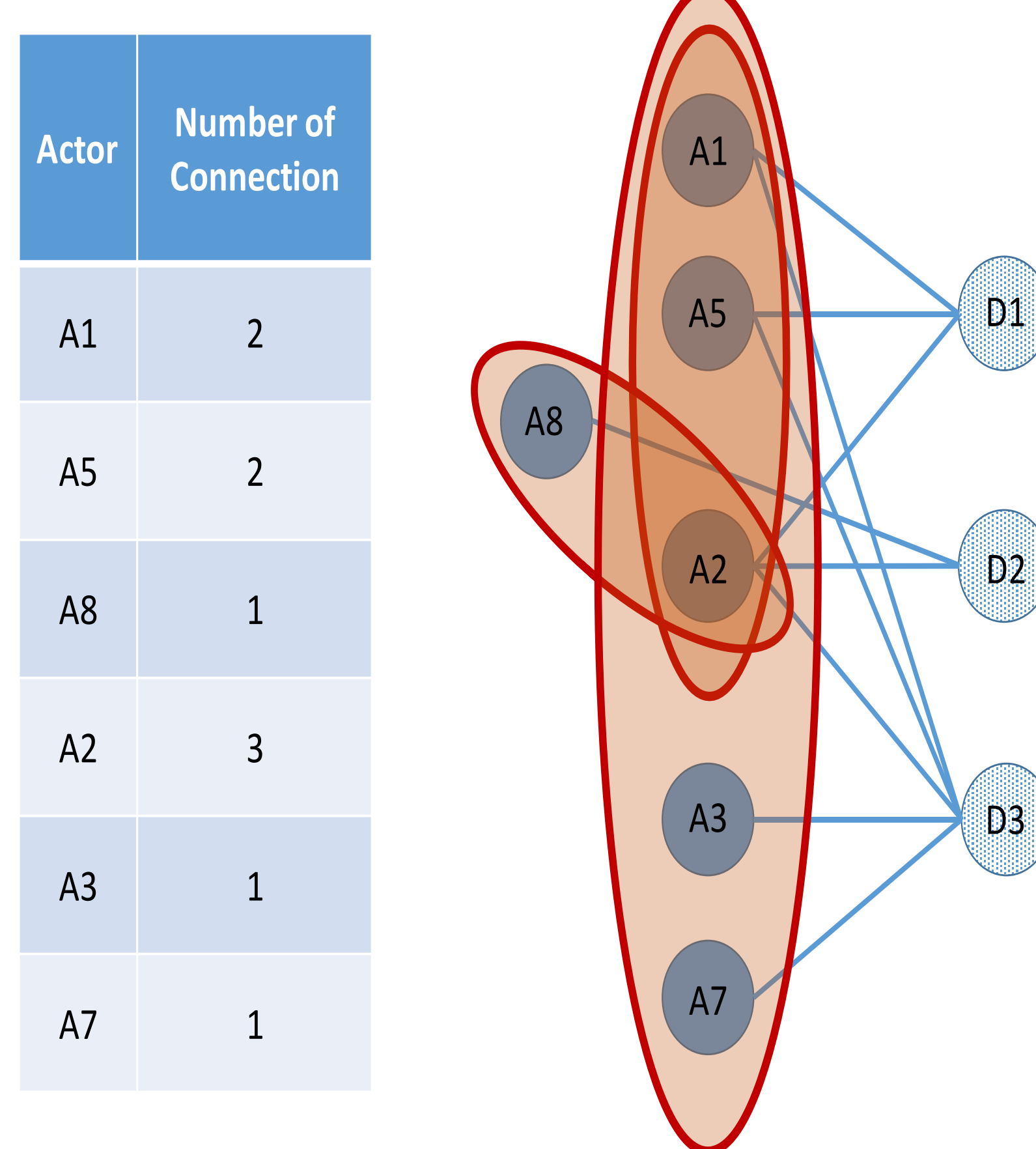


FIGURE 2: SHOW DATA LINKS BY VENN-DIAGRAM

For a given number of actors, which is marked Na, if we would like to examine the maximum possible number of each group, the following formula can be written:

$$Cl_{max} = 2^{Na} - 1$$

In order to optimize the security of the IT system, the importance of certain relationships must be known. Importance of a relationship describes how many actors are able to access any data structure through a link. The relationship of interest increases by the number of actor who is able to access a given link and consequently the amount of shared objects which are available through the connection as well. The significance of the relationship which defined as (Cj) is based on the size of actors in that particular group (Na) and the number of their available shared objects (Nd).

$$Cj_i = Na_i \cdot Nd_i$$

Relative to the total system weight of a connection (ji) can be defined as follows:

$$Cp_i = \frac{Cj_i}{\sum_{i=1}^n Cj_i}$$

The different importance of data and its represented information, such as commercial, personal data, or minor, public data should be taken into consideration in the model. It is characterized by a factor of data relevance (Dj) which is assigned to each data. In this case, the context of the formula is changed as follows:

$$CDj_i = Na_i \cdot Nd_i \cdot Dj_i$$

The resulting weight of the data and relations (Vli) can be defined as follows:

$$Vl_i = \frac{CDj_i}{\sum_{i=1}^n CDj_i}$$

This value indicates a quantity proportional to each group size and importance of accessible data and information. High quantity means that numerous users have access to numerous information, so the level of a successful attack probably causes more damage on information assets. This value can be used to identify the vulnerable points of an IT system.

EXAMINATION THE IMPORTANCE OF GROUPS TO IT SECURITY

Our examined model is based on the structure of College of Dunaujv ros. The college is a state educational institution. Different organization units have been built in order to make effective work. The access of different data and information (including critical, sensitive information) is under supervision. Each organization unit uses individual systems. The data access of these units is implemented by different eligibility groups.

	Students	Instructors	Leader instructors	Administrative staff (HR)	Administrative staff (SIO)	Administrative staff (FO)	Security staff	System admins	Domain admins
CI	1	2	3	4	5	6	7	8	9
Na	3000	88	11	7	15	22	10	12	6
Nd	3	3	4	4	4	3	2	6	8
Cj	9000	264	44	28	60	66	20	72	48
Dj	0,001	0,1	0,3	0,5	0,3	0,5	0,6	0,8	1
CD	9	26,4	13,2	14	18	33	12	57,6	48
VI	4%	11%	6%	6%	8%	14%	5%	25%	21%

VULNERABLE LEVEL OF MAIN USER GROUPS OF COLLEGE OF DUNA JV ROS

The significance of groups in terms of IT security is determined by the number of external attacks and relations of information in the group. In this paper (taken into account accessible information systems of groups, determined various metrics) we mapped with a model that these groups can affect the information assets when a negative event occurs.

Being aware of this level of risk, may help designing the protection of users, user groups and the total IT system.

CONCLUSION

The table of vulnerable levels represents well the threat level of actors for the entire system. Students are considered as the lowest risk factors, while administrators and domain administrators are high threat in terms of data security. Accordingly, the threat level of actors is directly proportional to the vulnerable level. It can be observed that the weight of the data and relations (Vli) is strongly influenced by the number of actors and data accesses: domain administrators have all eligibility in the IT system and the administrators (because superiority of its headcount) can cause more damage to the information assets. It can be seen in the table that in terms of data access, system administrators and domain administrators are the most dangerous for the entire system. In contrast to these groups, students represent the lowest vulnerable level. The threat level is multiplication of the number of actors (Na), available information systems (Nd) and factor of data relevance (Dj). The significance of groups in terms of IT security is determined by the number of external attacks and relations of information in the group. In this paper (taken into account accessible information systems of groups, determined various metrics) we mapped with a model that these groups can affect the information assets when a negative event occurs. Being aware of this level of risk, may help designing the protection of users, user groups and the total IT system.