

# Examination of the vulnerable levels of user groups based on an IT security model

Tibor Ujbanyi\*, Jozsef Katona\*, Attila Kovari\*

\* College of Dunaujvaros/Institute of Computer Engineering, Dunaujváros, Hungary  
 ujbanyit@mail.duf.hu, katonaj@mail.duf.hu, kovari@mail.duf.hu

**Abstract**— 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.

## I. INTRODUCTION

When we talk about information security, it is important to understand the meaning of the term. IT security is the protection of the managed data and the management system. At this point, it should also be noted that IT security is not the same as information security. The latter one relates to protect treated data in all communication systems (written, oral, electronic), while IT security is only protect the IT system. When we talk about defense and security in IT systems, we have to know the components of the system: hierarchical structure, the links between internal components, subsystems and wider environment. [1]

Attacks against information systems can be divided into two groups: external and internal attacks. External attacks arise from people who do not belong to the organization and do not have access rights to the IT system. These attacks have implemented on the Internet, through network connection by intruders. The danger of internal attacks is taken to occur if the intruder has an appropriate access privileges to the IT system. In addition, the intruder has some important information that will facilitate the penetration. He knows the structure of the system and he has physical access to the computers and network devices. He knows the internal policy and his co-workers, so he also knows which data is really important to the organization. He knows the location of data, so it is easier to access critical information and potential vulnerabilities can be more easily used. But in the context of internal attacks, it should be noted that not all attacks are done deliberately; it may also be done in some cases where the employers brings in a virus or other security threats unwittingly to the system.

When information leaking out, we can represent all of the possible contacts between the supposed perpetrators and important traces. The case can be analyzed with a graph based evaluation method. It can be performed a prior analysis for primary targets of psychological manipulation (social engineering) based attack. Primary targets may be people or information. These attacks try to find the weak spot of the system, take advantage gullible and vulnerabilities of users. [2] Primary targets of attack

of the IT systems are users and applications that have access to more information in the system. The descriptions of access to information like connections are modelled by graphs. [3, 4]

In case of attacking IT systems, those users and applications have high priority that have an access to lots of data. If a user group or application get access to the most of the critical data, then these factors poses the greatest threat to the IT system event of successful internal attack. If a user or a user group have access to large sets of data, the protection of these groups affects the data security. The number of connected (cooperative) users has to be limited. It is necessary because if the user is a member of many related groups, the achievable data increases largely. If a user group which access data treated by other user groups, then infection of this group can spread to several other groups. Therefore, due to an attack, these user groups are important in order to protect the IT system. As described above, it can be concluded that in terms of IT security, the importance of groups has to be quantified in some way highlighting the number, size and data access connections of different groups that affect IT security. [1]

The complete IT system of user groups, client and server applications, data as shared information as well as the links between them has to be established with taking into account that the system does not contain major significant points in terms of attack, which points are likely to be more exposed to such attacks. An IT system designed in this manner can be provided a higher average of security level.

## II. 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 types of graphs are bipartite graphs. [5, 6]

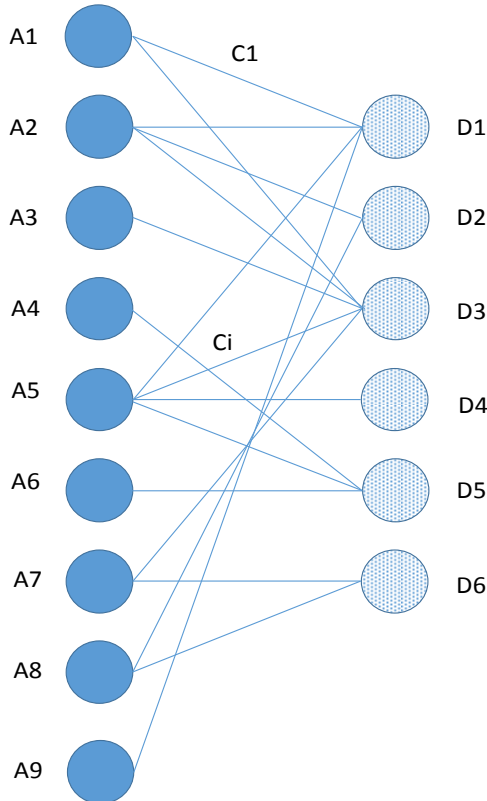


Figure 1. Graph model of actors, shared objects

The mathematical representation of these graphs when A and B are disjoint sets:

$$G = (A, B) \quad (1)$$

The edges of the graph are an implicit or explicit communication channel produced by links. Because the actors can access a shared object or a group of shared objects represented by links a sub-group of actors can establish the sub-graph of the entire graph according to Figure 2.

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. [5, 6]

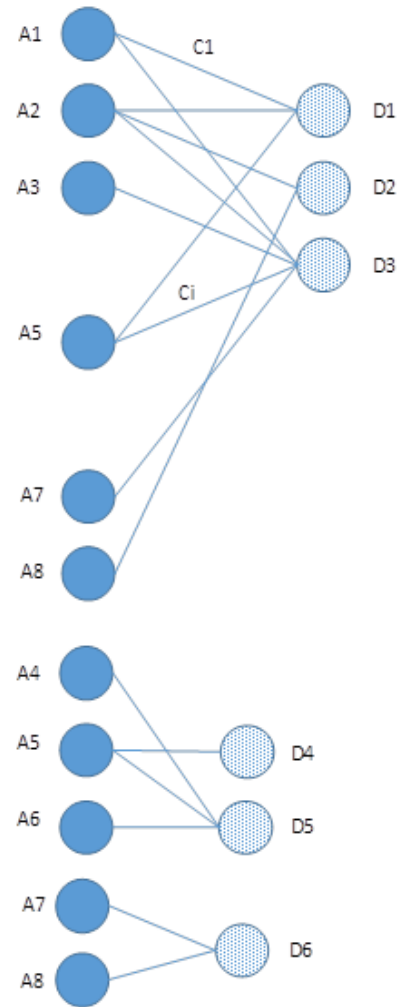


Figure 2. Sub-graphs of actors and shared objects

| Actor | Number of Connection |
|-------|----------------------|
| A1    | 2                    |
| A5    | 2                    |
| A8    | 1                    |
| A2    | 3                    |
| A3    | 1                    |
| A7    | 1                    |

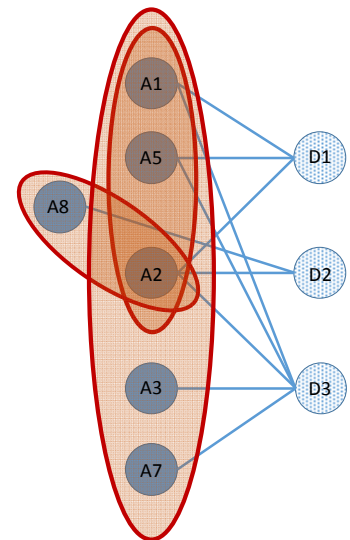


Figure 3. Show data links by Venn-diagram

According to the examination of IT security by the methods described in [2], the investigation of cases of “leaked” information among isolated groups by privileges of certain data access in case of a prey on some kind of security vulnerability occurs can be done based on the Venn-diagrams. Using Venn-diagrams, information leakage among groups could be established. This information leakage can be realized between groups along information channels by the overlap of among certain groups. If we would like to illustrate the descriptive information channels between certain actors and their sets, it can be done by a Venn-diagram as shown in Figure 3.

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

$$Cl_{max} = 2^{N_a} - 1 \quad (2)$$

The maximum numbers of possible groups are numerous in spite of the fact that there is a few actors only. To be able to minimize the security risk of the system, it is necessary to determine the significant level of each connection. As illustrated in Figure 2, the data links represented in Venn-diagram can be specified by a set representation which can be shown in Figure 3. In this representation the segments of sets mean the relationships between the various groups.

The relationship of groups is shown in Figure 4. This is a simplified way to represent relationships of the data structure in bipartite graphs as shown in Figure 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 ( $C_j$ ) is based on the size of actors in that particular group ( $N_a$ ) and the number of their available shared objects ( $N_d$ ).

$$C_{j_i} = N_{a_i} \cdot N_{d_i} \quad (3)$$

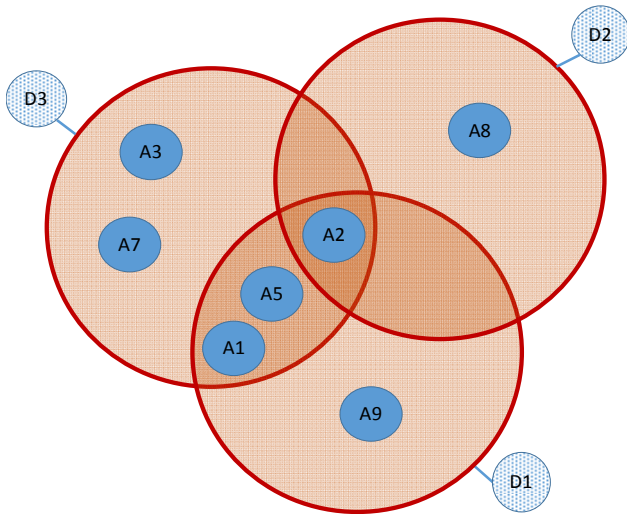


Figure 4. Show groups by sets

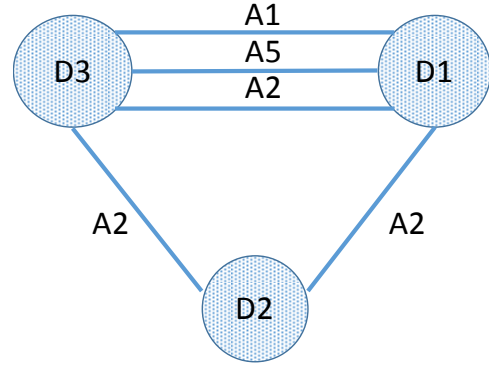


Figure 5. Link's net

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

$$Cp_i = \frac{C_{j_i}}{\sum_{i=1}^{Cl} C_{j_i}} \quad (4)$$

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 ( $D_j$ ) which is assigned to each data. In this case, the context of the formula (3) is changed as follows:

$$CD_{j_i} = N_{a_i} \cdot N_{d_i} \cdot D_{j_i} \quad (5)$$

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

$$VI_i = \frac{CD_{j_i}}{\sum_{i=1}^{Cl} CD_{j_i}} \quad (6)$$

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.

### III. EXAMINATION THE IMPORTANCE OF GROUPS TO IT SECURITY

Our examined model is based on the structure of College of Dunaujváros. 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.

TABLE I.  
VULNERABLE LEVEL OF MAIN USER GROUPS OF COLLEGE OF DUNAÚJVÁROS

|    | Students | Instructors | Leader instructors | Administrative staff (HR) | Administrative staff (SIO) | Administrative staff (FO) | Security staff | System admins | Domain admins |
|----|----------|-------------|--------------------|---------------------------|----------------------------|---------------------------|----------------|---------------|---------------|
| Cl | 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%           |

HR: Human Resource Management

SIO: Student Information Office

FO: Financial Office

We defined some groups in the table and along with this the number of actors (Na). The number of information systems accessible by actors can also be read from the table. This value describes that how many actors are able to access any data structure through a link. Factor of data relevance (Dj) is a estimated value that describes the importance of accessible information in terms of IT security. There is a scale in the table ranging from 0 to 1, which describes the significance of accessible data set by groups.

Each group has a different eligibility level. Employers' group of the College can be divided into three groups: instructors, students and non-instructors. In terms of data access, the group of non-instructors can be divided into more subgroups: technical and administrative staff. Members of technical staff are system administrators, mechanics and security staff. Administrators of institutes and secretaries belong to the administrative staff.

In the three groups, the groups of students have the least privilege. The group achieves Neptun and Moodle systems (read and write permissions where necessary). The administrative staff has already higher privileges. This staff achieves different registers, central document management (MonDoc, library database) or individual and institution network drives. The group of technicians can be divided into subgroups; maintenance staff has minimal eligibility as they can use computers and achieve some registers. They have not got access to the important internal systems. System administrators are the most significance staff in terms of data access. They manage the groups and access rights, allow and deny permissions from users who have been given personalized settings. The group of system administrators also can be divided into domain and local administrators' group. Domain administrators give more authorities to local administrators.

#### IV. SUMMARY AND 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 (VIi) 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.

#### REFERENCES

- [1] Ross J. Anderson, *Security Engineering, A Guide to Building Dependable Distributed Systems*, 2<sup>nd</sup> Edition, Wiley, 2008
- [2] Kevin D. Mitnick & William L. Simon, *The Art Of Deception*, John Wiley & Sons, 2006.
- [3] Louise E. Moser, "Graph homomorphisms and the design of secure computer systems," *Proceedings of the Symposium on Security and Privacy*, IEEE Computer Society, 1987, pp. 88-96.
- [4] Xinming Ou, Wayne F. Boyer, Miles A. McQueen, "A scalable approach to attack graph generation," *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 336-345.
- [5] Trudeau, Richard J., *Introduction to Graph Theory*, New York: Dover Pub, 1993.
- [6] Gross, Jonathan L., Yellen, Jay, *Handbook of graph theory*, CRC Press, 2004.