Diagram of Security

Marek Vysoký*
Department of Computers and Informatics
Faculty of Electrical Engineering and Informatics
Technical University of Košice
Letná 9, 042 00 Košice, Slovakia
mvysoky@lundegaard.sk

Abstract

In this thesis I describe model called Diagram of security [1], which extends existing UML models, specifically Deployment diagram, which is intended for modeling architecture of network systems and it is a model of cooperation between hardware and software components. In my thesis I describe the security requirements of company managers and I suggest methodology of modeling of network systems in terms of security. Diagram of security is comprehensive tool, which will examine network systems to find weaknesses in terms of security and will estimate correct security risk in the deploying or existing network system.

The proposed Diagram of security includes attributes of security[2], by which I define algorithms for detect weaknesses and critical path in terms of security. The result is the determination of potential risk threats of attacks and ability to respond to incidents. Other proposed algorithms analyze the actual security situation and respond to incidents indicating the range of potential attackers and the ways through which the attack could be carried out. Designed security model is endowed by real data from various components such as servers, firewalls, workstations and various other components and by regular transmission of data model is updated and is thus still image of the modeled system. Thesis objectives are handled programmatically with documenting the function for selected examples. Also I pay attention to cost analysis associated with increasing levels of security. I define algorithms that allow estimating the financial costs and the costs associated with implementation of security policy in the organization. With this thesis I introduce the knowledge level of security to the design of network systems architecture.

*Recommended by thesis supervisor: Assoc. Prof. Milan Šujanský. Defended at Faculty of Electrical Engineering and Informatics, Technical University of Košice on September 9, 2010.

Vysoký, M. Diagram of Security. Information Sciences and Technologies Bulletin of the ACM Slovakia, Vol. 4, No. 1 (2012) 39-43

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Unauthorized access; K.4.2 [**Social Issues**]: Abuse and crime involving computers

Keywords

security, risk management, graph algorithm, deployment diagram, security modeling, hacking, forensic analysis, UML, network systems

1. Introduction

In the analyzing the actual state of risk management [3] and modeling security I found, that in the area of risk management are defined different methodologies and methods for calculating impact of environment in terms of security, which I specifically mapped and described in the thesis. I found the lack of tools, which able to exactly model and analyze the status of the security of network system and through which it is possible to detect potential threats and impacts of attacks from users and which could be applied graph algorithms to identify weaknesses in terms of security.

2. Thesis objectives

Assessing the actual state in modeling security the following objectives were defined in the thesis:

- define a model to determine the boundaries of network system and security risk factors of network system,
- create definition of Diagram of security, allowing mathematical and graphical interpretation of the modeled system in terms of network security and will be based on the definition of UML model, namely the Deployment diagram,
- define the attributes of Diagram of security that make it possible to evaluate security properties of modeled elements,
- define analysis algorithms to detect vulnerabilities and critical path in terms of security and determine the potential risk of threats of attacks and ability of system to respond,
- implement a basic cost analysis addressing the security policy. The result of the analysis will be to serve as a basis for management decisions and enable risk management to decide on further investments in security features and method of system development.
- define algorithms that analyze the real situation and react to incidents and to determine potential attackers and paths through which the attack could be carried out,
- create a methodology of cooperation of Diagram of security with the deployed network systems and an interface

allowing the updating of attributes of model based on real information from modeling environment[2]. The model is subsidized by real data from various components such as servers, firewall, workstations and various other components, where regular sending data to the interface of the model and keeps the actual image of the modeled system,
- create a software tool that allows modeling network systems and allows application defined algorithms and which provides a graphical interface for creating a Diagram of security.

3. Diagram of security

Basic concepts defined for the Diagram of security[1]:
Entity – is a network element (firewall, network drive, switch), or computing equipment (workstation, server, PDA, notebook).
Data source – represents the data storage (database, file server, the content repository). In many cases, the data storage is deployed on entity and could be included in a set of entities, but for modeling is important for us to determine the path to data sources and the risk their abuse.
Connection – is a relation between two entities or between an entity and data source.
User – is a person who uses the entity and uses data sources. User access to data sources across the various network elements, or by computer (workstation, PDA ...) and uses the data sources accessed to achieve their goals.
Diagram of security – is a network model to modeling and evaluating the security attributes of the modeled system in terms of security.
Diagram of security is defined as $Db = (U, E, \alpha, \beta, \omega, \delta)$ where:
U – is a finite set of users of the system of internal and external environment.
E – is a finite set of entities (desktops, firewalls, servers ...).
DS – is a finite set of data sources (databases, data storage, file systems ...).
$\alpha : (ExE) \rightarrow 1|0$ – is a projection defining the relation between entities. The connection between the entities exists if the result is 1.
$\beta : (ExDS) \rightarrow 1|0$ – is a projection, defining the relationship between entities and data sources. The connection between the entity and data source exists if the result is 1.
$\omega : Ux(ExE) \rightarrow 1|0$ – is a projection, which determines access rights to the user entity. When a user has access result is 1 otherwise 0.
$\delta : Ux(ExDS) \rightarrow 1|0$ – is a projection, which determines access rights to the user entity. When a user has access result is 1 otherwise 0.
Access Vector – determines user's access to entity or data source. The values are from set $(0, 1)$, or may be specifically named rights such as$(read, insert, update, delete)$.
Risk Vector – determining the risk of disclosure of an entity or data source for user. Values are set $(low, middle, high)$ and we can determine the risk in connection with the allocation of access.

3.1 Graphical representation of Diagram of security

Diagram of security extending UML diagram (Deployment Diagram). Fig. 1 is a simple example of Diagram of security.

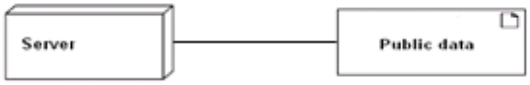
The user is from set U and is represented by symbol:

The entity is from set E and is represented by symbol:

Data source is from set DS and is represented by symbol:

Projection α - connection between entities is represented by the edge:

Projection β - connection between entities and data sources is represented by the edge:



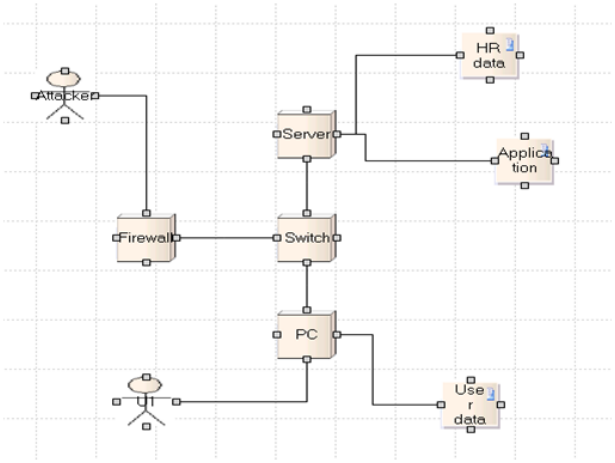


Figure 1: Example of simple Diagram of security.

3.2 Security attributes of entities

Entity software security Ess - is a coefficient that determines the credibility of the software and the operating system.
Entity number of incidents Eni - value, which is a weighted average of security incidents on the entity.

3.3 Security attributes of data sources

Data sensitivity $DSds$ - is a coefficient that determines the classification of data and determines the importance of data and the level of damage in the event of misuse, alteration or deletion.
Data source software security $DSss$ - is a coefficient that determines the credibility of the software and the operating system, which is used directly for the data source.
Data source cryptography DSC - is a coefficient, which we determine by comparing the reliability of cryptographic algorithms.
Number of incidents $DSni$ - value, which is a weighted average of security incidents on the data source.

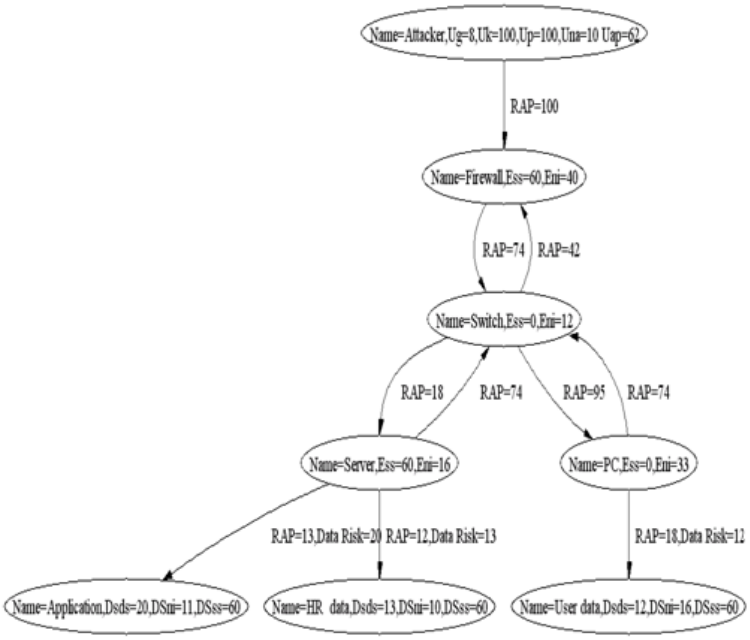


Figure 2: Diagram of availability obtained from Diagram of security.

3.4 Security attributes of connections

Transfer cryptography TC - a coefficient, which we determine by comparing the reliability of cryptographic algorithms used for data transfer over the channel between entities and data sources.
Data sensitivity Tds - is a coefficient that determines the classification of data and determines the importance of data and the level of damage in the event of misuse, alteration or deletion.

3.5 Security attributes of users

User goals Ug - is a coefficient, which determines the motivation of the attacker or user of system, performs an attack or incident cause.
User knowledge Uk - evaluation parameter, which determines the ability of IT, education and the ability to make attack.
User power Up - parameter specifies the technical equipment that a user can use to implement attacks.
User number of access Una - parameter determined by the total number of access in the modeled system, or frequency of use of computing resources in the network systems.

4. Algorithms used Diagram of security

4.1 Algorithm of analysis availability and breaking software defense

Algorithm of analysis availability and breaking software defense brings security risk rating, which is the input for the methodology of risk management[4]. Analysis availability determines the place, where the user of the system has access and what risk there is in his access to relevant information. Fig. 2 shows the result of analysis of the algorithm availability and breaking software defense and shows the result of decomposition of Diagram of security to Diagram of availability. Fig. 2 shows us the available data sources and entities for attacker. The edges shown risk of breaking defense RAP and on the edges leading to a data source is the risk of data access (Data Risk). In the thesis I described each algorithm in detail and also provide examples of results taken from the software tool.

4.2 Algorithm analysis of security incidents in Diagram of security

Algorithm analysis of security incidents decomposes Diagram of security to Incident index diagram to ensure awareness of the potential increased risks to the individual entities and data sources. The higher the weight of incidents, the risk is increased because of increased security activity in the entity, or data source. This may indicate a break defense, or installed software bugs.

4.3 Algorithm of analysis of cryptographic level

Algorithm of analysis of cryptographic level decomposes Diagram of security to Diagram of availability indicating the cryptography level of the connections. For the evaluation we have a clear rule the higher the level of encryption, the encryption is secure.

4.4 Indication of the level of cryptography in Diagram of security

Algorithm indicates level of cryptography in Diagram of security at the edges, representing connections. The result shows the level of encryption in the modeled system.

4.5 Algorithm for finding path with the highest risk of breaking

Applying this algorithm we get risky path for each user and we need to prepare implementation of corrective measures or strengthening the security policy.

4.6 Algorithm for finding path of weak encryption

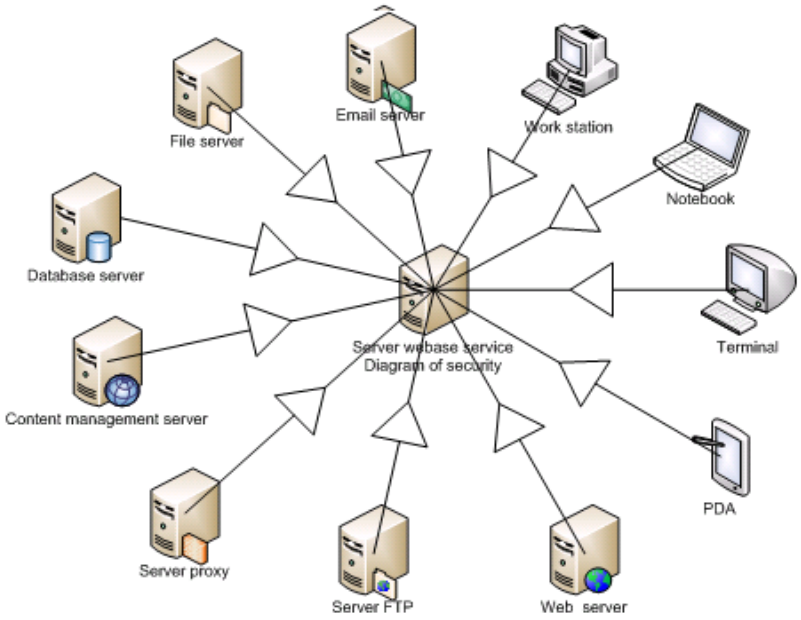


Figure 3: Transmission of the information from entities.

The algorithm shows us the critical path in terms of cryptographic level for each user. The edges are marked with the encryption level. We can analyze the outcome of the algorithm and can increase level of security in low-encryption and application of encryption algorithms for different levels of network layer.

4.7 Algorithm for finding path of high occurrence of incidents

The algorithm appears risky path from the perspective of increased security incidents for each user. The edges are marked with risk of breaking defense. Increased weight of incidents indicates a threat of attack, or indicates an error of installed software.

4.8 Algorithm for finding of potential attackers

Applying the algorithm for finding of potential attackers we get a result which determines a set of potential attackers in response to the incident in one of the entities, or data source.

4.9 Algorithm evaluation of the financial costs

Applying the algorithm evaluation of financial costs we determine the financial costs required to improve level of security. The result of evaluating is the financial costs for each entity, data source and connection.

4.10 Algorithm evaluation of the financial costs by finding critical path

For large systems, it is not possible for financial reasons to increase global security. The algorithm analyzes risky places and path in modeling system and the result of evaluating the financial costs in critical path.

5. Application diagram of security in monitoring security in real systems

To monitor the real security, I propose a model of communication, which interacts with the modeled objects, and receives and updates their parameters in Diagram of security. Fig. 3 is a simple outline of a possible interaction between objects and the web service. Centralized web-based service allows data transfer between objects and updating the diagram with real data. The client application must include:
- Security log analysis - to determine the incidents and security events.
- Detection of user access - identifying a user name and identification data, determining the number of visits and analyze its behavior in terms of security.
- Detection of installed software - a complete software detection and detection newly installed software.
- Transfer to a Web service must be authenticated and the data must be transferred securely using encryption algorithms.

6. Conclusion

Definition of Diagram of security allows modeling of network systems of small and large scale and to define the boundaries of the modeled system. In the definition of a Diagram of security, I defined the basic elements of a Diagram of security, which are entities, data sources and connections and their security attributes[2]. For users, I define the security attributes such as user goals, knowledge, power and number of access used for risk analysis of the threat of possible attack. The definition of graphical representation of a Diagram of security was based on UML model, namely the Deployment diagram. I have defined algorithms that evaluate network systems and allow analyzing and identifying weaknesses in terms of security. In response to the objectives I have implemented a software tool which I have implemented the algorithms described in the thesis. Outputs of the analysis show the graphical results of the implementation of algorithms, such as example on Fig. 1. The software tool includes a web service that allows collection of real information from the modeled network systems.

References

[1] M. Vysoký, *Príspevok k riešeniu bezpečnosti distribuovaných informačných systémov,Písomná práca k dizertačnej skúške*. Košice: TU Košice, Máj 2005.

[2] M. Vysoký, *Specification of security attributes in the diagram of security*. TU Košice: INFORMATICS'2009 - International Scientific Conference on Informatics, 2009.

[3] G. Stoneburner and F. Goguen, A., *A Risk Management Guide for Information Technology Systems*. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf: NIST Special Publication 800-30, 2008.

[4] B. Bakley, E. McDermott, and D. Geer, *Information Security is Information Risk Management*. New Security Paradigms Workshop, ISBN:1-58113-457-6, 2001.

Papers by the Author

Vysoký, M.: Príspevok k riešeniu bezpečnosti distribuovaných informačných systémov, písomná práca k dizertačnej skúške, Technická univerzita Košice, Máj 2005.

Vysoký, M.: Diagram of security, SCYR 2009, 9th Scientific Conference of Young Researchers, Košice, May 13, Faculty of Electrical Engineering and Informatics, Technical University of Košice, 2009

Vysoký, M.: Specification of security attributes in the diagram of security, INFORMATICS'2009 - International Scientific Conference on Informatics, November 2009

Vysoký, M.: Debugging of Parallel Programs, Acta Electrotechnica et Informatica No. 3, Vol. 6, 2006, ISSN 1335-8243, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Slovak Republic