Security level quantification and benchmarking in complex networks

Vesselin Tzvetkov
vesselin.tzvetkov@vodafone.com
Vodafone GmbH, Alfred-Herrhausen-Allee 1, 65760 Eschborn, Germany

***Abstract-* The security of complex networks with multiple elements is very difficult to evaluate and characterize by numbers. The interaction between the network elements, the different layer topologies and the numerous features makes the security quantification almost impossible. On the other side, the lack of security benchmarking is very problematic for the budget and invests allocation by companies. Numerical economical indexes for the costs and potential benefits are used to set the budgets. The security is not be quantified and it cannot be mapped to these economical indexes, thus the budget is not set objectively. This paper suggests a novel framework for quantification of network security, thus security benchmarking. The relative vector expresses the different layers, physical connections, operation risk, and human resources. The benchmark is relative and not absolute value, which is an indirect indication for the security. The relative security vector maps to economical values and helps the management to take the decisions. The suggested framework extends the common standards like ISO 27000, BSI, ITIL, which characterize single network elements or processes in corporations. This framework is the missing link between the security standards, subjective expert analysis and the monetary instruments. The benchmarking is not saying if a system is secured, then it gives a relative indirect comparison between systems.**

***Index Terms-* Network security, security benchmark, security vector, security quantification, BSI, ISO 27000.**

I. Introduction

The management of company has significant problems dealing with IT security. On the one hand, the security is not delivering directly any productive features and therefore, it is only an indirect revenue generator. For example, installing a firewall is not increasing the network performance. On the other hand, the security is very important for the corporation because of: the government requirements for privacy of the personal data, the impact of losing corporate knowledge, critical customer information, intellectual property etc.

Currently, the corporations invest billions for network security improvements without the ability to link them numerically to security level. The management is working with numerical values, like Rate of Return [7], OPEX [6] or CAPEX [5], which are instruments to determine the investment and return. Without a quantification of the network security, the budgets for security cannot be set properly. There are simple questions with difficult answers, like how security is changing depending of the investment?

Furthermore, a problem is the monitoring of the security level over the years. For example: the last year was installed firewall, is there a need for second firewall this year? How this new investment will improve the security?

The risk of wrong configuration during operation increases with each additional device. For example: huge number firewalls increase the risk of wrong administration. At some point, there will be so many mistakes at operation than the total security will decree dramatically. Clearly, the complex systems have higher risk of functioning in the wrong way, which decrees the security. Typically, to overcome this, more staff is hired for crosschecks. More staff reflects in higher risk of insider attacks, which decreases the security of the system.

The security is complex topic and cannot be expressed in absolutely values. The reason is that this will require evaluation of million of scenarios and knowledge of all possible vulnerabilities. This is practically impossible.

For this reason in this paper are targeted to steps. First, an abstraction to higher degree is made. Second, benchmark for indirect quantification is suggested, which has sense only in comparison between the enterprises. The result is an indirect indicator of the security with respect of different layers security, operational error risk and human resources. The idea is not to create an absolute value expressing the security risk in probability value, than relative benchmark used only in comparison. In the same way as the economical values are only indirect indicators of the success of corporation.

The calculation must be transparent and open standard in order to facilitate the comparison between the corporations. Close standards, called black boxes, do not really give any result of the security. This is very important property. Let us take an example of the financial indexes. There will be no use of revenue announcement if its calculation procedure is different in every company. The strength of the finance indicators is that all participants calculate them in the same manner. Therefore, the values can be compared otherwise the numbers will be useless. The security benchmark must be treated in the same way, thus it must be announces for all stock participants. The security index and the financial results can be disadvantageous of some corporation in bad condition but they are information right of all shareholders. Therefore, the corporation must be committed to announce the results in the same manner, as the stock requires for the financial indexes.

This work can not exchange the analysis of the security by professionals. It targets only the extend it.

II. Target

The target is to create a set of numerical values (vector) describing the security of network considering the relation between the network elements, thus network topology. The result vector can be abstracted to single value, so it can be mapped to economical values of corporation. The value is relative and an indirect indication for the security making sense only in direct comparison. The vector, also called security benchmark, must have following properties:

- Expressing the risk of successful attack by outsider and insider.
- Express the security relations between the components.
- The complex systems have a higher risk of failures, thus the values must consider the risk of wrong operation leading to vulnerabilities.
- Duplication of security information increases the security risk. For example: every backup copy of private data directly increases the risk of successful attack on it.
- Consider that operation costs increase when adding hardware and software.
- Base on the already existing certifications, like BSI [1], ISO 270xx [4] etc.

III. Related works

The ISO/IEC 270xx [4] is a set of best practice recommendations on an overall Information Security Management System (ISMS), like processes in corporation, responsibilities, services and management. The corporation can certificate on ISO/IEC 270xx. The BSI Standard 100 [14] specification focuses more practical definition in the same aria as ISO/IEC 270xx. The BSG Grundschutz [1] gives a concrete recommendation on single network element, like server, router, firewall etc. It specifies the basic requirement for the proper protection of the element. In the same manner, the Common Criteria [2] is certificate for the secure qualities of certain product. The ITIL [3] defines the organization of services and processes without emphasizing on the security. The existing standards give practical advices on the organization. The corporation can implement and obtain certificates assuring the quality of the structures. The certificates and implementation give Boolean answer (true or false), if the corporation has passed this test.

These standards do not give any numerical result of networks security and do not create score or benchmark, which is the target of this paper. The deployment of standards increases the security of the network and reflects in the created benchmark. The novel framework is link between the mentioned standards and the economical values.

IV. Security Vector

A network consists of numerous elements, like routers, switches, web-servers, desktop-PC etc. An element is a logical independent system and not limited to physical device. A network element is for example Load balancer consisting of multiple physical devices. Furthermore, multiple elements can be running on a single physical device. For example: on a server is running a firewall and in the same time web server. In this sense, an element is abstraction technology dependent (see V). The exact level of abstraction can vary and is out of subject in this short paper.

Every element has its vector for characterization containing of 4 dimensions: *security level* against successful attack, *management interface security* level, risk of *wrong operation* and *required resources*.

Security level is vector with component for every security relevant OSI layer. There are six directly relevant layers: physical layer (1), data layer (2), network layer (3), transport layer (4), presentation layer (6) and application layer (7). The session layer is not security relevant. Typically, the network and transport layer are gathered in the same feature set in the devices. For example Access Lists treat network (IP) and transport (TCP/UDP) parameters in the same command, like an example Cisco IOS[8] ACL:

```
access-list 107 permit udp any host 82.82.10.1
range 16384 32767
```

The transport and network layer are characterized with single value in the same manner. The vector for the *security level* can be notated as:

$$\lfloor p_1\, p_2\, p_{3-4}, p_6\, p_7 \rfloor, \; p_n \in (0,1) \subset \Re$$

The *p* represents the security of the OSI layer where the subscript is the layer. The *p* values are between zero (0) and one (1) where zero means secure and one unprotected system. The means of the vector components is:

p_1 describes the physical security of the system, thus how easy is the gain access to the device. There are server rooms with restricted access for example.

p_2 represents the link layer security, for example protections against MAC [10] spoofing.

p_{3-4} represent the typical firewall security, thus access list on IP and TCP/UDP level. They are implemented on routers, firewalls and hosts. For example, Windows OS firewall feature includes statefull inspection firewall.

p_6 is the presentation layer, like TLS/SSL.

p_7 describes the application security. For example, web server content must be resistant against attacks, like cross-site scripting (XSS) [11].

The *risk of wrong operation* is single value expressing the complexity of the system. In general, a complex system tends to have high risk by the operation. Even the system is high secured it have high risk of wrong operation, which decreases the effectiveness of the system. This is parameter can be linked to the qualification and number of the staff. The values is noted as $\{o, o \in (0,1) \subset \Re\}$. The zero (0) means no risk and one (1) means very high risk.

The third parameter is the *operational resources*. Every network element requires configuration, planning etc. It is very important to express the resources needed for management since less staff increases the security risk. The operational resources value is greater then zero (0) without upper limit, thus $\{r, r \in (0,+\infty) \subset \Re\}$. The value is not direct absolute expression of number of administrators, engineers etc. The value has sense only in comparison between the corporations and development in the years, thus it is a relative. It can be mapped to real numbers of persons only by comparing. For example: a firewall requires more resources than switch.

Every element has management interface at application layer, like telnet, ssh or web interface. The security of the *management interface* is expressed with $\{m, m \in (0,1) \subset \Re\}$. The zero (0) means secure and one (1) means no security at all.

The security vector for single element A (superscript) is denoted as:

$$\begin{pmatrix} \left[p_1^A p_2^A p_{3-4}^A, p_6^A p_7^A \right] \\ o^A \\ r^A \\ m^A \end{pmatrix},$$

V. Security Vector Initialization

The security vector of a network element must be initialized before any further calculation. The vector is technology depended and vendor independent. The vendor specific vectors can raise a strong competition and possible values manipulation by the competitor. This will mislead to the framework's target to calculate the total risk reflection of the interaction between multiple system elements. The values for the different technologies must be publicly set and constant for all calculations.

The *security level* is calculated as number of vulnerability at this layer for this technology to the total number of vulnerabilities at this layer. The number of vulnerabilities can be obtained for public database, like [12, 13]. If the element is not working at certain layer, then the values is set to zero. A firewall is less vulnerable than web server and consequent will have lower (better) security level. Alternative, the security level may be set using general expert knowledge, less for firewall (secure) and high for web server (no secure). Important is the values to be plausible and constant in all calculations.

The risk of *wrong operation reflects* to operation complexity of one system. It is a very subjective values but the system can be classified to elements with low (0.1), medium (0.5) and high complexity (0.9). The operational resources are set low (0.1), medium (0.5) and high (0.9).

The *security of management interface (MI)* expresses the local policy and the highest security level protecting the management interface. For example, if firewall protects the management interface, then the MI is at equal to firewall security level. If additional, there are username and password protection, then the security of MI increased by serial connection with the security of the application for authentication (see VII). The element protecting the MI is typically firewall at the border and centralized authentication and authorization server.

Different methods can be used for the initialization, but at this stage of research, the author considers this one as best one.

VI. Interaction between the Elements

The communication topology depends of the OSI layer, thus it changes significantly at different layers. The security issues can be found at every layer. It must be discussed which topology must be considered for the security vector.

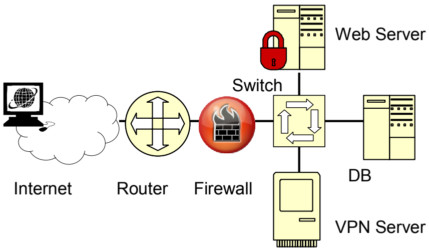

Figure 1. Simple network at physical connection

An example of simple network at physical layer is shown at Figure 1. The firewall is connected to internet thought router. The switch is connected to: Web server, Database server (DB), VPN server and firewall (link layer). This is considered to be common scenario. There is not information of any IP relation and the information exchange by the applications then only wires.

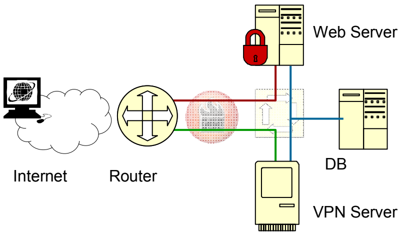

Figure 2. Link layer structure

The same network is presented at link layer at Figure 2. The colored lines are VLAN connections [9]. The switch and firewall are transparent for link layer, thus they are shown transparent. The link connections have different topology then the physical. The web server and router are connected in VLAN *red*. The VPN Server and router are in VLAN *green*. The web server, VPN server and DB are connected in VLAN *blue*, called backend connection. The web server and VPN server have each two logical interfaces serving the front and back end.

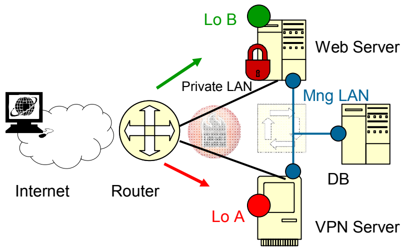

Figure 3. Network layer communication

Figure 3 shows the same network at network layer. The IP domain is quite different from the link layer. The web server and VPN server have two logical interfaces with private IPs (black line and blue line at the figure) and additionally one public local loopback IP (green and red circle at the figure). The DB server has only one private IP at the interface. Static route to the local loopback IPs are set at the router (green and red arrow).

At the application layer, the topology is again different (s. Figure 4) The Web and VPN server communicate to the Internet and the DB server. The web and VPN do not communicate to each other. There are no other application layer communications.

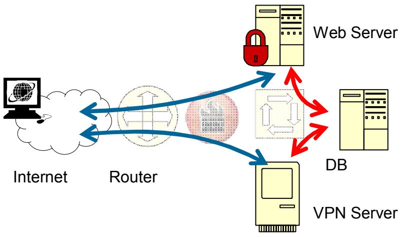

Figure 4. Application layer topology

The topology is quite different at OSI layers and there are security issues at every layer. The physical connection is the precondition for all other possible topology.

The security vector is calculated on the basis of the physical layer. The argument for this can be summarized as:

- The higher layer are mostly result of device configuration and can be influenced by attacker. For example: an attacker can easily change the routing table or IP addresses which changes the topology. The physical connection can be changed only by physical attack, which is not typical.

- The topology on application layer is not always univocal, thus having only one solution. There can be different descriptions depending of the abstraction of the application layer.
- The higher layer topology becomes very complex in large networks.
- The physical topology is univocal and easy to express.

Further in this frame work only the physical topology is considered.

VII. Security Vector Operations

Mathematical operations can be performed with the security vectors in order to expressed the result network vector. There are two operations for combining vectors: *parallel* and *serial* connection. The *serial* connection means that the two elements are following each other. For example, this is the router connected to the firewall as at Figure 1. The elements can be installed on the same physical device as in the case of the web server with firewall (red lock) at Figure 1. The result vector *AB* of *serial* connection on elements *A* and *B* is:

$$\begin{pmatrix} \left[p_1^A p_2^A p_{3-4}^A, p_6^A, p_7^A\right] \\ o^A \\ r^A \\ m^A \end{pmatrix} * \begin{pmatrix} \left[p_1^B p_2^B p_{3-4}^B, p_6^B p_7^B\right] \\ o^B \\ r^B \\ m^B \end{pmatrix} = \begin{pmatrix} \left[p_1^{AB} p_2^{AB} p_{3-4}^{AB}, p_6^{AB} p_7^{AB}\right] \\ o^{AB} \\ r^{AB} \\ m^{AB} \end{pmatrix}$$

The security level for serial connection is calculated as:

$$p^{AB} = \frac{p^A}{n} + \frac{p^A . p^B}{n+1},$$

where the n is the position form outside perspective, thus the first device has $n=1$, the second has $n=2$ etc. The n is weight coefficient which stress the devices near to the outside as more important for the security. The motivation for this equation is that first device has influence on protecting the second. The first element practically protects the second, since the attacker must pass the first element to access the second. This is the reason why the company set firewall at the border if possible. The multiplication $p^A \cdot p^B$ shows than the first device protects the second.

The weight coefficients give a fair way to compare networks with low and high number of devices. The devices at back positions are less important to the front devices. Otherwise, companies with many devices will be always with poor security because of the number of devices even protected.

The operation risk means also probability of failure in one of the two systems, thus also OR of independent exclusive event:

$$o^{AB} = P\left(o^A \cup p^A\right) = o^A + o^B - o^A \cdot o^B$$

The required resources for the operation are not probability then addition of the required resources, thus:

$$r^{AB} = r^A + r^B$$

The addition does not represent absolute the number of operators and engineers. There are synergy effects, management tools etc. This linear addition can be, as already set, only relatively compared to other systems. The security level of the management interface is:

$$m^{AB} = \frac{m^A + m^B}{2}$$

This is the mean of the security level. The motivation is subjective since there is no correlation between the topology and the management structure.

Two network elements can operate *parallel* when the traffic is proceed either by one or the other device. This is *CD* for elements *C* and *D* as:

$$\begin{pmatrix} \left[p_1^C p_2^C p_{3-4}^C p_6^C p_7^C\right] \\ o^C \\ r^C \\ m^C \end{pmatrix} \oplus \begin{pmatrix} \left[p_1^D p_2^D p_{3-4}^D p_6^D p_7^D\right] \\ o^D \\ r^D \\ m^D \end{pmatrix} = \begin{pmatrix} \left[p_1^{CD} p_2^{CD} p_{3-4}^{CD} p_6^{CD} p_7^{CD}\right] \\ o^{CD} \\ r^{CD} \\ m^{CD} \end{pmatrix}$$

The security level of *parallel* connection is the addition of both values, thus:

$$p^{CD} = p^C + p^D$$

The attacker can chose the first or the second element. The security decreases (the values become high) by the both probabilities.

The topology does not influence the operational risk and resources then the element's properties. Therefore, the operation risk, security of management interface and required resources are calculated in the same way as by serial connection.

VIII. Calculation Procedure

The result security vector is calculated starting from outer entry point, thus Internet and Internet. If there are multiple entry points, there will be multiple results vectors. The summarized result vector is the parallel connection of all entry point's vectors.

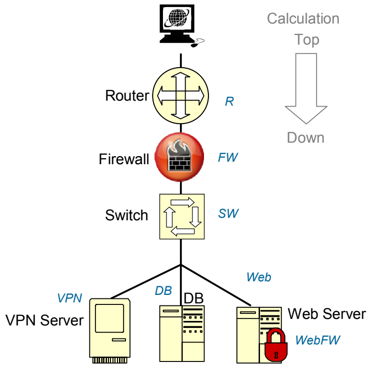

Figure 5. Graph for security vector calculation

The network can be presented in graph structure in order to simplify to calculation. There is different graph for every entry point. The security vectors of the elements for internet and internet entry points may be different. The security properties of the elements depend of internet or internets access typically. For example a small residential router (SOHO) has a different properties on WAN and on the LAN interface, so there will be two security vectors, thus for internet and intranet. Theoretically, there can be different vectors for every interface, but the author considers it as insignificant for the results.

The graph of the simple network given at Figure 1 is presented at Figure 5. The blue italic abbreviation near the element is used also as superscript for the security vector values. The calculation is made top to down. There is only one entry point in this simple network and the result can fast calculated as:

$$\begin{pmatrix} \left[p_1^R\, p_2^R\, p_{3-4}^R\, p_6^R\, p_7^R\right] \\ o^R \\ r^R \\ m^R \end{pmatrix} * \begin{pmatrix} \left[p_1^{FW}\, p_2^{FW}\, p_{3-4}^{FW}\, p_6^{FW}\, p_7^{FW}\right] \\ o^{FW} \\ r^{FW} \\ m^{FW} \end{pmatrix} * \begin{pmatrix} \left[p_1^{SW}\, p_2^{SW}\, p_{3-4}^{SW}\, p_6^{SW}\, p_7^{SW}\right] \\ o^{SW} \\ r^{SW} \\ m^{SW} \end{pmatrix} *$$

$$* \left\{ \begin{array}{l} \begin{pmatrix} \left[p_1^{Web}\, p_2^{Web}\, p_{3-4}^{Web}\, p_6^{Web}\, p_7^{Web}\right] \\ o^{FW} \\ r^{FW} \\ m^{FW} \end{pmatrix} * \begin{pmatrix} \left[p_1^{WebFW}\, p_2^{WebFW}\, p_{3-4}^{WebFW}\, p_6^{WebFW}\, p_7^{WebFW}\right] \\ o^{WebFW} \\ r^{WebFW} \\ m^{WebFW} \end{pmatrix} \oplus \\ \oplus \begin{pmatrix} \left[p_1^{DB}\, p_2^{DB}\, p_{3-4}^{DB}\, p_6^{DB}\, p_7^{DB}\right] \\ o^{DB} \\ r^{DB} \\ m^{DB} \end{pmatrix} \oplus \begin{pmatrix} \left[p_1^{VPN}\, p_2^{VPN}\, p_{3-4}^{VPN}\, p_6^{VPN}\, p_7^{VPN}\right] \\ o^{VPN} \\ r^{VPN} \\ m^{VPN} \end{pmatrix} \end{array} \right\}$$

The Figure 6 shows an example of network with multiple intranet entry points and one internet entry point. There is one remote office (superscript with "ho"), and two local LANs (superscript with "int1/2"). At every intranet, there are two entry points - computer and IP telephone. There are total six (6) intranet and one (1) internet entry points. The internet vector is denoted as A und intranet security vector as B. The both vectors can have the same values for elements with one access interface.

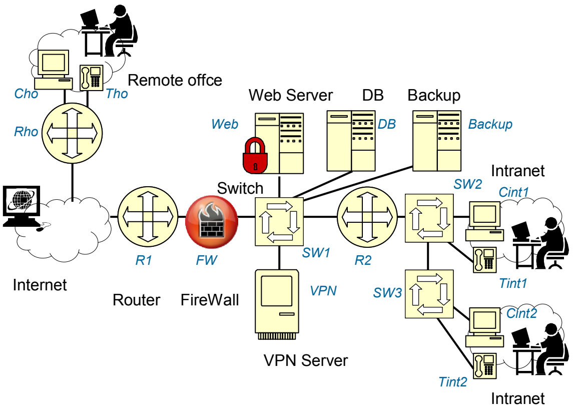

Figure 6. Network with multiple entry points

The result security vector E is the parallel sum of all vectors, thus:

$$\mathrm{E} = \mathrm{B}^{Sum} \oplus \mathrm{A}^{Sum}$$

The internet entry vector is:

$$\mathrm{A}^{Sum} = \mathrm{A}^{Rro} * \left(\mathrm{A}^{Tro} \oplus \mathrm{A}^{Cro}\right) \oplus \mathrm{A}^{R1} * \mathrm{A}^{FW} * \mathrm{A}^{SW1} * \\ * \begin{pmatrix} \mathrm{A}^{Web} * \mathrm{A}^{WebFW} \oplus \mathrm{A}^{DB} \oplus \mathrm{A}^{VPN} \oplus \mathrm{A}^{Backup} \oplus \\ \oplus \mathrm{A}^{R2} * \begin{pmatrix} \mathrm{A}^{SW2} * \left(\mathrm{A}^{T\,\mathrm{int}\,1} \oplus \mathrm{A}^{C\,\mathrm{int}\,1}\right) \oplus \\ \oplus \mathrm{A}^{SW3} * \left(\mathrm{A}^{T\,\mathrm{int}\,2} \oplus \mathrm{A}^{C\,\mathrm{int}\,2}\right) \end{pmatrix} \end{pmatrix}$$

The intranet entry points are expressed as:

$$\mathrm{B}^{Sum} = \mathrm{B}^{ro}_{SumTel} \oplus \mathrm{B}^{ro}_{SumCom} \oplus \mathrm{B}^{\mathrm{int}1}_{SumTel} \oplus \\ \oplus \mathrm{B}^{\mathrm{int}1}_{SumCom} \oplus \mathrm{B}^{\mathrm{int}2}_{SumTel} \oplus \mathrm{B}^{\mathrm{int}2}_{SumCom}$$

$$\mathrm{B}^{ro}_{SumTel} = \mathrm{B}^{Tro} * \mathrm{B}^{Rro} * \begin{pmatrix} \mathrm{B}^{Cro} \oplus \mathrm{B}^{m} * \\ * \begin{pmatrix} \mathrm{B}^{SW2} * \left(\mathrm{B}^{T\mathrm{int}1} \oplus \mathrm{B}^{C\mathrm{int}1}\right) \oplus \\ \oplus \mathrm{B}^{SW3} * \left(\mathrm{B}^{T\mathrm{int}2} \oplus \mathrm{B}^{C\mathrm{int}2}\right) \end{pmatrix} \end{pmatrix}$$

$$\mathrm{B}^{ro}_{SumCom} = \mathrm{B}^{Cro} * \mathrm{B}^{Rro} * \begin{pmatrix} \mathrm{B}^{Tro} \oplus \mathrm{B}^{m} * \\ * \begin{pmatrix} \mathrm{B}^{SW2} * \left(\mathrm{B}^{T\,\mathrm{int}\,1} \oplus \mathrm{B}^{C\,\mathrm{int}\,1}\right) \oplus \\ \oplus \mathrm{B}^{SW3} * \left(\mathrm{B}^{T\,\mathrm{int}\,2} \oplus \mathrm{B}^{C\,\mathrm{int}\,2}\right) \end{pmatrix} \end{pmatrix}$$

$$\mathrm{B}^{\mathrm{int}1}_{SumTel} = \mathrm{B}^{T\mathrm{int}1} * \mathrm{B}^{SW2} * \begin{pmatrix} \mathrm{B}^{C\mathrm{int}1} \oplus \\ \oplus \mathrm{B}^{m} * \mathrm{B}^{Rro} * \left(\mathrm{B}^{Tro} \oplus \mathrm{B}^{Cro}\right) \oplus \\ \oplus \mathrm{B}^{SW3} * \left(\mathrm{B}^{T\mathrm{int}2} \oplus \mathrm{B}^{C\mathrm{int}2}\right) \end{pmatrix}$$

$$\mathrm{B}^{\mathrm{int}1}_{SumCom} = \mathrm{B}^{C\,\mathrm{int}\,1} * \mathrm{B}^{SW2} * \begin{pmatrix} \mathrm{B}^{T\,\mathrm{int}\,1} \oplus \\ \oplus \mathrm{B}^{m} * \mathrm{B}^{Rro} * \left(\mathrm{B}^{Tro} \oplus \mathrm{B}^{Cro}\right) \oplus \\ \oplus \mathrm{B}^{SW3} * \left(\mathrm{B}^{T\,\mathrm{int}\,2} \oplus \mathrm{B}^{C\,\mathrm{int}\,2}\right) \end{pmatrix}$$

Even the calculation seems to be complex it can be optimized for computer calculation. There are only two operation: serial and parallel addition. For every entry point the graph must be drawn where the entry point is on the top. The Figure 7 presents the graph for telephone of the remote office at Figure 6.

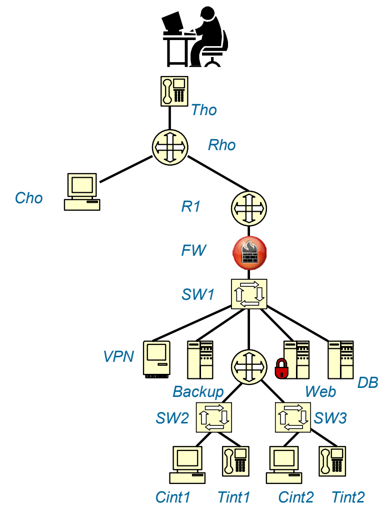

Figure 7. Graph for the network entry point

IX. ABSTRACTION THE SECURITY

The result security vector can be abstracted to single representative values, since the layer separation is complicated for non technical staff. The summary number of the security level is:

$$p = w_1 p_1 + w_2 p_2 + w_{3-4} p_{3-4} + w_6 p_6 + w_7 p_7 + w_8 m \ ,$$

where w is weight coefficient. The weight expresses that the security depends on the layer. Some layers are more typical for attacker then other.

The principle "the higher layer the more potential attacks" is implemented in this paper. The reason for this subjective assumption is that the higher layers have more remote accessible features, which increases the risk of successful attack. For example, physical access in server room is easy restricted. The application interface may be access per Internet all over the world. Based on this subjective knowledge, it is defined:

$$w_1 = 1,\ w_2 = 2,\ w_{3-4} = 3,\ w_7 = 4, w_8 = 5$$

The number of involved employees is unknown and therefore, the operational risk can not be related to the staff. For this reason, the ration of the operational risk to the resources is not considered in the general security index calculation, but is can be considered in future work based on this paper.

X. Simulation

The simple simulation is proof of concept and targets to demonstrate the property of the suggested benchmark. To facilitate the understanding, it is calculated only one layer in a very simplified calculation.

There are only two device types: high secured and low secured device. The high secured is a firewall with security level of 0.1. The low secured device is server with security level of 0.7. In every case, the security vector is calculated for 2 devices and than step-by-step increased to 20 devices in total keeping the same connection schema. The number of devices is shown at the X-axis. The security level is shown at Y-axis. Figure 8 presents the results.

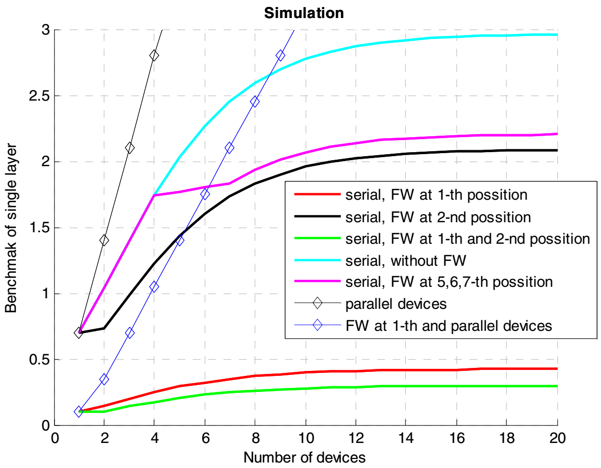

Figure 8 Simulation results

The first simulation (red line) all devices are serially connected. A firewall (high secured) is at the first position. Servers (low secured) are added at all following positions. The security level increase with every added device, thus the security becomes worst. Because there are weight coefficients, the devices at back have less importance. Therefore, the curve does not increase to infinity (poor security). It is important to compare to the other following cases.

In the second case (black line), the devices are serial connected and the firewall is at the second position. All other positions are servers. Practically, the firewall position is changed to first case. The security becomes poorer then the first case. This is logical since the firewall is at second position. A possible hacker can gain asses to the server at the first position. This server could have valuable information how to gain access to the other server and in this way to facilitate an attacker. The firewall at second position does not protect the first server and this is not desirable.

In the third case (green line), there are serial connection where at first two positions are firewalls. The security is better (low service level) that the first case. This is the result of the two firewalls instead of one. It must be stressed, that the security do not improved linear. The security is not twice better that with single firewall. The reasons are the weight coefficients dependent on the position.

The fourth case (blue line) is serial connection of server without any firewall. The security decreases rapidly. At some level of 15 following devices, it becomes constant. The security cannot decrees more since the following device are almost unimportant of the network protection.

In the next case (magenta line), there are firewall at 5th, 6th and 7th position of serial connection of elements. They improve insignificantly the security, even three of them, comparatively to firewall at first position. Here manifests the principle that a firewall at front is better than multiple firewalls at the backside of the network.

In the sixed case (black line with rhombus), there are parallel servers. The security decrees quite rapidly with every added device. The security is worst that the serial connection of server (blue line). This is logically since an attacker has a free choose of all servers in parallel connection. In the serial connection, it must gain access server by server.

In the last example (blue line with rhombus), there are firewall protecting parallel connection of servers. The security is better then the previous case, since the firewall protects the server. The security is better then serial connection of servers with less then 6 elements. The probability of successful hack of the network behind the firewall increases with number of the devices. At some point (in this case by six devices), the single firewall cannot compensate the lack of security at all the backend devices.

XI. Conclusion and Future work

The method suggests simple and practical method of network security benchmark, which reflects the security scenarios. It must be underlined that the network carrier should announce publicly the results of evaluation. The companies with poor results will sure try to avoid any announcement, since this will decrease their reputation. It cannot be expected that the companies will announce this values voluntarily. The security vectors must be announced obligatorily in the same manner as the companies participating on the stock announce theirs financial result.

Some companies will try to tune the topology to obtain better security score even their real security is poor. This cannot be avoided by any method. In the same manner, some corporation play with their accounting result only to improve to financial reports nut in deed are bankrupted.

The suggested method can be further develop and probably improved. This work is considered as staring of the discussion and not its final stage.

References

[1] “IT-Grundschutz Catalogues”, http://www.bsi.de
[2] “Common Criteria for Information Technology Security Evaluation”, http://www.commoncriteriaportal.org
[3] “IT Infrastructure Library”, ITIL v3, http://www.itil.org/
[4] ISO/IEC 27000, http://standards.iso.org/ittf/PubliclyAvailableStandards
[5] Capital Expenditure - CAPEX, http://www.investopedia.com/
[6] Operating expense - OPEX, http://www.investopedia.com/
[7] Rate of return, http://en.wikipedia.org/wiki/Rate_of_return
[8] Cisco IOS, http://www.cisco.com/go/ios
[9] Virtual LAN (VLAN), IEEE 802.1Q, http://www.ieee.org/
[10] Media Access Control address (MAC), IEEE 802.3, http://www.ieee.org/
[11] Cross-site scripting , http://en.wikipedia.org/wiki/Cross-site_scripting
[12] The Open Source Vulnerability Database, http://osvdb.org/
[13] National Vulnerability Database, http://nvd.nist.gov/
[14] “BSI Standard 100”, http://www.bsi.de