Investigation of intrusion detection and intrusion prevention systems in eHealth hospital network

Maria V. Nenova

The fast growth of the requirements in the eHealth area leads to the problem of protection of personal data and the need of secure transmission via communication channels. The investigated and proposed in the paper solution may be used in a healthcare facility's corporate network where the patient sensor network is expected to send to the processing units the required in the fewest possible number of data packages, using just one of its sensor to make a connection. Another fact to be considered is that package size must be optimal so as not to incur a loss of large and significant information. The solutions proposed may be used for intrusion protection of networks, whose units must receive as little load as possible from the software products used and from the communication process. This is mostly required for units, whose task is to process or store a large volume of diverse information at the same time, as well as for units, whose task is to process and visualize information by using specialized software products.

Изследване на система за детекция и предотвратяване на интрузии в мрежа за електронно здравеопазване (Мария В. Ненова). *Непрекъснатото увеличаване на изискванията в областта на електронното здравеопазване води до проблема за защита на личните данни, както и необходимостта от сигурното им предаване по канала за връзка. Изследваното и предложено в доклада решение може да се използва в глобалната здравна мрежа, където се очаква, че сензорът на пациента изпраща на обработващите елементи, възможно най-малко на брой пакети от данни, като се използва само един сензор, за да се осъществи връзка. Друг факт, на който е необходимо да се обърне внимание е размера на пакета, който да е оптимален, така че да няма големи загуби на важна информация. Предложените решения могат да се използват за защита от проникване в мрежата, чиито елементи е необходимо да имат минимално натоварване, както от софтуерните продукти, така и от самия процес на комуникация. Това е необходимо, най-вече за устройства, чиято задача е да обработва или съхранява голям обем разнообразна информация по едно и също време. Това е в сила и за устройства, чиято цел е да обработва и визуализира информация чрез използване на специализирани софтуерни продукти.*

Introduction

The term e-Health entered popular use in late 1999 [1]. It brings together public healthcare, medical informatics, healthcare service provision and information by using state-of-the-art information and communication technology.

The purpose of e-Health is to solve to underlying yet fundamentally different issues. Most countries are facing the dilemma of how to maintain high level of healthcare vis-à-vis price increases in the healthcare services and specialized healthcare facilities. At the same time the underpopulated areas of developing countries suffer from abnormally high patient-physician ration, which stands at 1 500:1 for Latin America and South Asia, 5 000:1 for Northeast Asia, and 20 000:1 for Central Africa [2]. Both issues are solved by the introduction of e-Health.

For most countries, setting up an electronic health platform is an important step towards provision of more efficient and better quality healthcare services going forward. However, implementation of e-Health also needs appropriate software protections to ensure data security for patients and stakeholder institutions.

The focus herein is on this particular issue, namely protection against attacks (intrusions) on the corporate network of any healthcare facility taking part in e-health.

The main objective is to propose, following

analysis of the potential intrusion sources, a functional model of network protection via use of a Snort system.

The information collected and processed by a tablet, laptop, or another device may be saved in the database of the e-Health platform. Then it may be used not just to diagnose the patient, but also generate emergency medical care signals via the internet. The accessibility and mobility of the devices used by patients in their daily lives poses a challenge. [3].

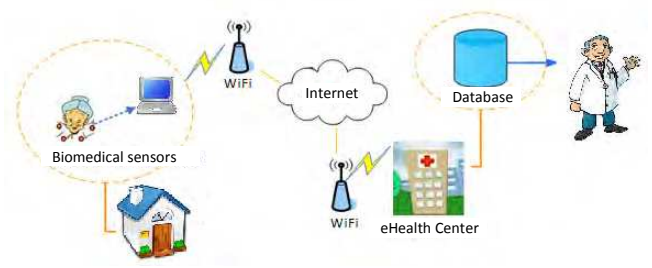

Fig.1. General view of e-Health.

Introduction of electronic storage and exchange functions for registries, health dossiers, case histories, etc., which contain personal data and health information, requires protection of such information, since it is easy to intrude.

Intrusion actions, which may be carried out, form just part of those familiar to and valid for the explored corporate network All of them jeopardize confidentiality of patient information and their medical dossier. The data transmitted from and to the sensor networks communicating with the servers, the data from and to transition devices performing the calculation and processing of the information collected, are also jeopardized. Unobstructed access to the eHealth system by patients, physicians and other parties in the eHealth network, is also under threat.

Specific software and protection system are required to protect the network from unauthorized access and intrusions. Once an intrusion is detected, operation of a preventive action mechanism is required to start. The following systems are used to implement such actions:

Prevention

Intrusion Detection Systems (IDS) – These may include all devices, which automatically register, analyze, and give out signals about each unauthorized activity in the communication network. [4]

Intrusion Prevention Systems (IPS) – These systems activate intrusion elimination steps, if intrusion signal has been given. [5]

Such systems are extensively used in corporate networks.

Intrusion detection and prevention systems

Intrusion detection systems register any abnormal behavior in the communication network's traffic and determine whether such behavior constitutes intrusion. They are used to protect against threats of known and unknown origin, as well as to protect against network or system blocking. On their own such systems are not sufficient for the system's comprehensive protection.

Protection against known threats takes place based on a search for known intrusion models in the traffic and events. Protection against unknown threats takes place based on construction of hypotheses to categorize any events as threats by using artificial intelligence, expert systems, or adaptive traffic filtering by specialized software. Blocking protection takes place based on detection of attacks, which cause network overloading with redundant traffic.

What is characteristic of IDS systems is that the package filtering rules are used on the entire package content or on successive packages. Analyzed are both the header and the actual information carried by the package. Analysis aims to detect a row of symbols, which may result in the occurrence of intrusion if they end up in the network. Two methods of analysis are used:

Signature analysis – a method for searching predefined models (rows of symbols) in incoming packages.

Anomaly analysis – a method for detection of certain models (incoming order of packages) in the network traffic, which are predefined as intrusion carriers.

Package analysis may be performed real-time or after the package has been copied onto another port.

System Snort

Snort is an IP (Internet Protocol) based network system for intrusion detection developed on open source basis. It may be configured and operated in three different modes of operation:

- *Packet Sniffer* – In this format Snort is in a sniffing function, wherein packages in the network are read and visualized on the end use screen.
- *Packet logger* – In this function Snort is only used to detect and protect the packages, which are retransmitted in the network.
- *Network IDS* – Snort in a network system format for intrusion detection. This function is the most complex one and requires extra

configuration but it has the capability of being set in such a manner that client's specific needs.

- Snort may only be used in one of the above formats at a time.

The overall structure of Snort is presented on Fig. 2.

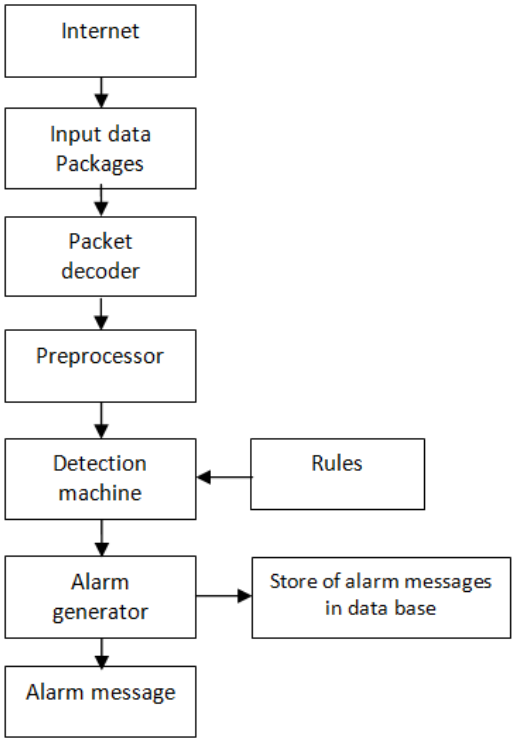

Fig.2. SNORT structure.

Once packages enter the system, they move on to the "package decoder". It prepares packages from different interfaces for processing. interfaces may be SLIP (Serial Line Internet Protocol), PPP (Point-to-Point Protocol), and others.

The preprocessor arranges and modifies the package data for the purpose of recovering their original appearance.

The track detection machines are tracing any tracks or signs of intrusions via a system of rules. The detection machine must operate real-time in order not to hold up traffic and thus destroy a number of user sessions.

Depending on whether intrusion has been detected, an alarm message may appear onscreen or be saved on the hard drive.

It may be recommended to use a Linux/UNIX operating system for the purpose of using Snort more flexibly. This would not result in any limitation of its capacity or operations, which may be performed with it.

Snort will not change, on the contrary, use of Snort in a Linux/UNIX environment is more extensively explored overall and offers more customization opportunities to the organization's particular needs. Snort is believed to be more stable and reliable in such types of environments.

To boost the economic efficiency of the proposed solution, namely, to use Snort as an IDS in background mode, it is also proposed to use Linux/UNIX operating system as basis for the application. The proposal was made based on the above factors.

Snort testing rules

The following rules were reviewed and explored in depth in order to determine Snort's functional capabilities: [6], [7], [8]

Rule #1:

```
Alert tcp any any -> any any
(content:"www.google.com";
msg:"Someone open google";
sid:1231213)
```

The above rule tracks the opening of the relevant page and when such action is taken it sends alarm via a message in the console or in a file. The package belongs to the TCP protocol, which may come from any IP address and is addressed to any IP address in the network. Sid (Snort Identification number) is the unique number of the generated rule. Since the rule is client-generated, its number is above 10, 000.

Rule #2:

```
Alert tcp any any -> 127.0.0.1
any (flags: A; \ack:0; msg:"TCP ping
is detected!")
```

The above rule tracks attacks and performs inspection of host activity. An Acknowledgement (A) flag of „0" value is used. The package belongs to the TCP protocol, which may come from any IP address and is addressed to the computer's local IP address. [9], [10]

Rule #3:

```
Alert tcp 192.168.1.33 any -> any
any (msg:"Traffic from 192.168.1.33
is detected!";)
```

The above rule tracks any TCP packages coming in from a certain IP address and addressed to any IP address in the network. If the event of such package, the following warning message appears.

Rule #4:

```
Alert tcp any any -> any any
(msg:"Possible exploit attack!";
content:"|90|"; nocase;)
```

The above rule tracks TCP packages from any IP address, which are addressed to any IP address in the network and contain a certain number (or text). In this particular case the tracking is for the appearance of a

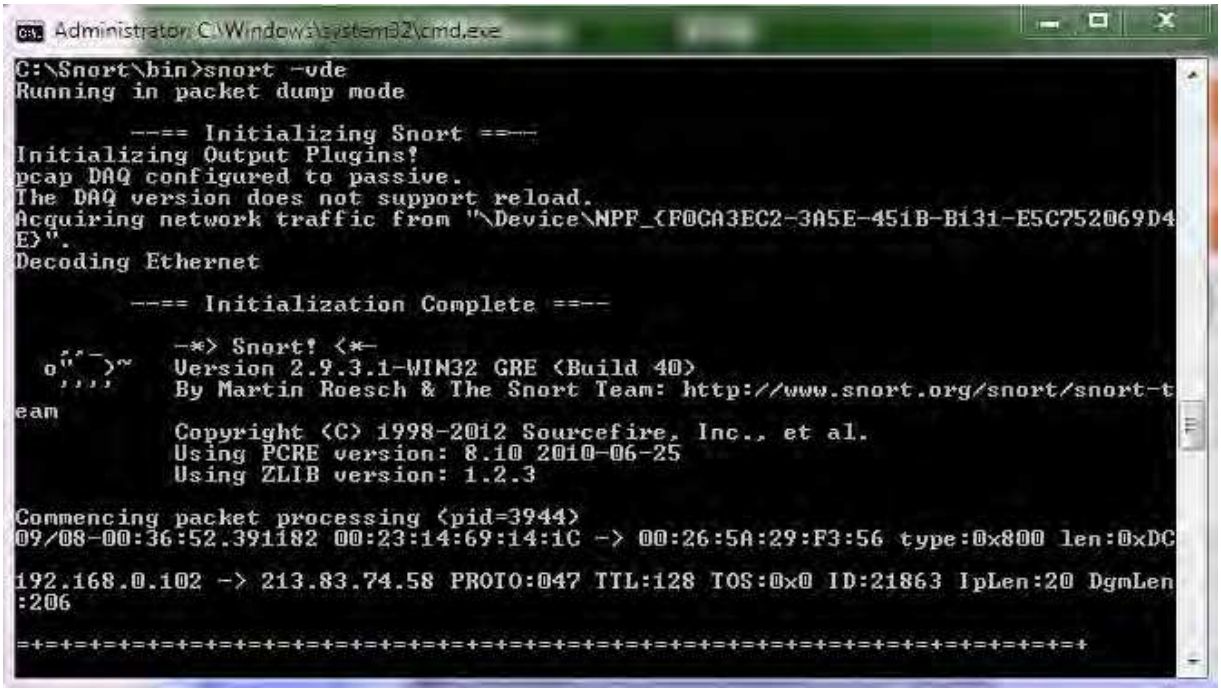

Fig. 3. Features a snort started in the Windows 7 operating system.

sequence of numbers in a hexadecimal code. In the event of such code, a warning message appears.

Simulations and experiments

The simulation program consists of a server, a switch, and clients of variable number.

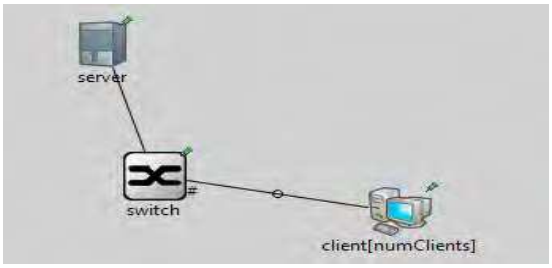

Fig.4. General model of the network with one server, switch and client.

The values from the simulation start with initial parameters are shown in Table 1. The values are derived for a variable number of clients.

Initial parameters:

On the client side:

- Time to make a connection – 10 [s];
- Order lead time – 2 [s];
- Number of orders for one connection made – 5; (Considering that the examined network is a corporate one and each client (BAN or another computer) would send to the server more than one data package for processing).
- Number of connections made by all clients – 5000 connections;

Table 1

Value of initial parameters for a variable number of clients

Initial parameters	**1** client	**8** clients	**20** clients
T (simulation time)	16605.78 [s]	1669.27 [s]	629.23 [s]
Simsec/sec (1 sim. sec. / 1 real-time sec.)	1.000992	1.000918	1.00012
Event/simsec (event / 1 sim. sec.)	3.33492	17.9689	54.3481

On the server side:

- Order processing lead time – 0.1 [s];

On the switch and channel side:

- Maximum number of packages queued – 20;
- Wait time – 10 [s];
- Delay in package transmission – 10 [ms];

The following are reported:

- Total time to conclude the simulation - T; We are interested in that one being minimal so that there would be optimal communication among network components.

Simsec/sec – averaged ratio of one simulation

second to one real-time second. This ratio must be approximately one (~1) on order to have real-time communication.

Event/simsec – averaged ratio of an event (connection making) to one simulation second; the purpose is for this ratio to be minimal in order for the simulation to support the real-time data transmission.

It follows from the reported results that a change in the initial parameters is required:

The parameters below were changed, as follows:

On the client side:

- Time to make a connection – 5 [s];
- Order lead time – 1 [s];
- Number of orders for one connection made – 1. (Considering that the examined network is a corporate one and each client (BAN or another computer) would send to the server more than one data package for processing);

On the server side:

- Order processing lead time – 0.1 [s];

On the switch and channel side:

- Maximum number of packages queued – 20;
- Wait time – 5 [s];
- Delay in package transmission – 5 [ms];

Once the simulation was started for the relevant number of clients, the following data were derived:

Table 2

Value of parameters following change in the initial ones

	1 client	**8** clients	**20** clients
T (simulation time)	12003.45 [s]	1018.61[s]	342.27[s]
Simsec/sec (1 sim. sec. / 1 real-time sec.)	1.00042	1.000027	1.000146
Event/simsec (event / 1 sim. sec.)	2.70023	65.215	132.3686

Following the conclusions made, the relevant changes were introduced in the parameters used for the simulations in order to achieve optimal real-time data transmission. *The following parameters were changed*:

On the client side:

- Time to make a connection – 5 [ms];
- Order lead time – 5 [ms];
- Number of orders for one connection made – 3. (Considering that the examined network is a corporate one and each client (BAN or another computer) would send to the server more than one data package for processing). We change the number of sent data packages since it would not be realistic that only one package would be sent throughout the entire communication.

On the server side:

- Order processing lead time – 0.1 [s];

On the switch and channel side:

- Maximum number of packages queued – 20;
- Wait time – 3 [s];
- Delay in package transmission – 4 [ms];

We now add a new parameter „Total memory limit"=32MB. This is the memory allocated for buffering outgoing vectors. It is commonly 16MB. By increasing it we ensure more efficient data processing during simulations. The main objective is to simulate data transmission in a channel with 2Gbps capacity. Once the simulation was started for the relevant number of clients, the following data were derived.

Table 3

Value of parameters following the second change in the initial ones

Initial parameters	**1** client	**8** clients	**20** clients
T (simulation time)	6870.34 [s]	793.53 [s]	291.81 [s]
Simsec/sec (1 sim. sec. / 1 real-time sec.)	0.99704	0.99953	1.000012
Event/simsec (event / 1 sim. sec.)	2.91221	49.6671	120.3331

After the last data set from the simulation were derived for a variable number of clients, the relevant conclusions and recommendations were made in previous section.

Conclusion

The solutions proposed herein for intrusion protection may be used in various corporate networks, not just those of a healthcare facility. The software products used may find extensive application since they also offer the option of modeling depending on the organizations' specific needs.

It may be used in a healthcare facility's corporate network where the patient sensor network is expected to send to the processing units the required in the fewest possible number of data packages, using just one of its sensor to make a connection. Another fact to be considered is that package size must be optimal so as not to incur a loss of large and significant

information.

The solutions proposed may be used for intrusion protection of networks, whose units must receive as little load as possible from the software products used and from the communication process. This is mostly required for units, whose task is to process or store a large volume of diverse information at the same time, as well as for units, whose task is to process and visualize information by using specialized software products.

The solutions proposed may also be used in corporate networks, which may invest in the creation of a high-speed communication network.

REFERENCES

[1] Website: **Error! Hyperlink reference not valid.**

[2] Vaswanathan, H., B. Chen, D. Pompili. Research Challenges in Computation, Communication, and Context Awareness for Ubiquitous Healthcare. IEEE Communications Magazine, May 2012, 0163-6804/12, pp. 92-99.

[3] website: http://www.wica.intec.ugent. be/research/ wireless-body-area-networks

[4] website: http://en.wikipedia.org/ wiki/ Intrusion_ detection_system

[5] website: http://en.wikipedia.org/wiki/ Intrusion_ prevention_system.

[6] website: ftp://petrinet.dvo.ru/pub/Vyatta/build-iso/pkgs/vyatta-snort/debian/my/snort_rules.html

[7] website: http://oreilly.com/pub/h/1393

[8] website: http://searchnetworking.techtarget.com/definition/SYN-scanning

[9] Boulis, A., D. Smith, D. Miniutti, L. Libman, Y. Tselishchev. Challenges in Body Area Networks for Healthcare: The MAC. IEEE Communications Magazine, May 2012, 0163-6804/12, pp. 100-106.

[10] Caldiera, J., J. Rodriques, P. Lorenz. Toward Ubiquitous Mobility Solutions for Body Sensor Networks on Healthcare. IEEE Communications Magazine, May 2012, 0163-6804/12, pp. 108-115.

Assist Prof. Maria V. Nenova *is with the Faculty of Telecommunications, Technical University of Sofia. Her scientific interests are in the field of adaptive signal processing, cryptography, security and standardization.*

e-mail: mariamnenova@gmail.com

Received on: 30.04.2015