A SECURE ACCESS SYSTEM TO MEDICAL DATABASES

Marian ALEXANDRU, Mihai ROMANCA

"Transilvania" University, Brasov, Romania

***Abstract**: In any distributed medical information system, health data security is very important. Therefore, data transmission is via secure protocols, for both smartcard and databases. In the current economical context is impossible to gather empirical data about a certain network, after deployment, because of high costs. Thus is imperative to design a simulation framework in order to be able to foresee any problems that might arise. The goal of this paper is to show the result of designing of healthcare network architecture and to create such a framework which is very important for a network interconnecting of healthcare facilities over vast geographical distances. It allows the study of key concepts, such as data security, scalability and modularity that are crucial in these types of networks.*

***Keywords**: Hospital information systems, Hospital network security, smartcard, VPN.*

1. INTRODUCTION

It is well known that medical institutions are implementing computer networks and hospital information system (HIS) technology. In the past years more and more healthcare institutions have adopted HIS integrated information systems to manage all the administrative, financial and clinical documents of a hospital. Such a system can enable: national sharing of information, improve patient doctor relationship, care provision and offer time, cost savings and convenience. An original approach for securing the access to a network that allows hospital actors to manage and have access to databases remotely is presented in this paper.

The paper (Tan *et al*, 2003) suggests the application of PKI (public-key cryptography infrastructure) and certificates to verify the authenticity of mobile users in the context of e-business and e-health information transactions. In (Xudong *et al*, 2005) the authors discusses the main consideration for integration of data, functions and workflow, among different and heterogeneous medical information systems in order to establish an enterprise hospital information system, and propose an architecture design system using digital neural network system in hospital. No aspects regarding the secure access and security of data are introduced. The paper (Scutaru *et al*, 2009) presents an original architecture, based on the concepts of SONA (Service Oriented Network Architecture) designed to take into consideration some important characteristics: scalability, integration with other existing hospital networks, remote and secure resource access, user friendliness, and complete data security. In (Cordos, 2008), the author proposes a three layer client-server architecture to be used in a HIS implementation for a Radiology Information System. The server resolves the problems of authentication, authorization, data security, privacy of access and protection.

Besides the proposed architecture, this paper includes a study of such a simulated network, using the Opnet Real Time Network Modeler. This section aims to validate the network's characteristics and functions according to its specifications.

2. ARCHITECTURE AND COMPONENTS

In response to the above mentioned healthcare system's needs we propose a complete central resource distribution system, aiming to be implemented at a national-level. This system ensures secure communications, remote resource access and personnel management.

As a proof of concept the architecture (Fig. 1) is designed in such a way that it can be easily integrated in any existing infrastructure and its scalability characteristics being heavily taken into consideration. The client component has a campus network topology and is represented in the Fig. 1 by the Windows XP Client machine; it aims to simulate the behavior of a resources access public terminal. The access to medical resources is granted based on a SmartCard or eToken solution type. These login methods provide secure access to resources based on digital certificates. The database is located at the server site, represented by the Windows Server 2003 machine. This structural component has a server farm topology and contains a Domain Controller that manages users and a database server that holds the actual resources. The client and server sites are interconnected through the Infrastructure component (SmartCenter and SmartConsole), which control the gateways (firewalls FW1 and FW2) that aggregate outbound traffic from all the sites. This component ensures data security of the traffic passing through either public or private networks. Firewalls are placed at the ends of the client and server, providing securecommunication between them through a VPN (Virtual Private Network) tunnel.

2.1 Server Component. In order to implement a system that takes advantage of a strong authentication method for secure network connectivity and data security, a central management system must be implemented. This system should control and organize smart card tokens throughout the institution. Without a well structured system, token based authentication solutions can be difficult or even impractical for organizations to adopt. The server, from an end-product point of view, contains the databases meant to be accessed by the clients. There are various ways of implementing these databases; SQL, MySQL and Oracle are some examples. These databases should be stored at the central location, in order to be reachable by all clients. Their structure can be distributed over multiple servers, but this brings up synchronization issues. A mechanism that ensures the correct placement of information into the database must be implemented, so that no redundant entries are present.

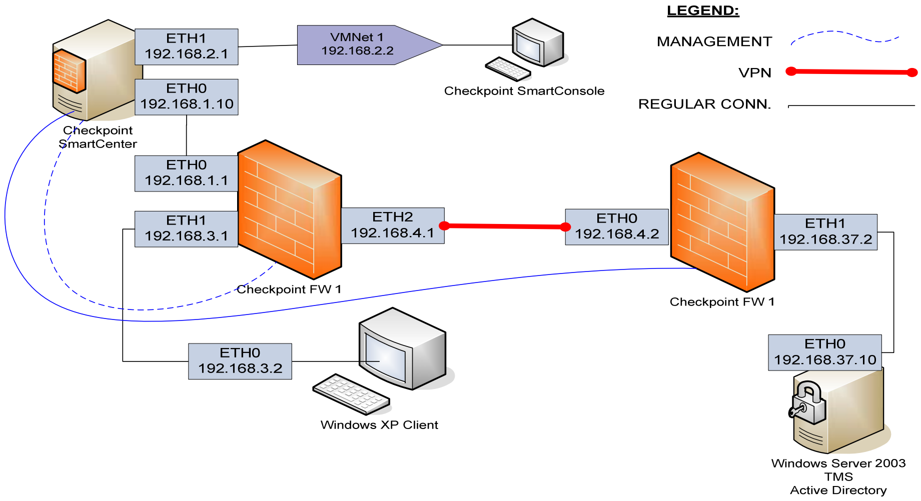


Fig. 1 Network Architecture Concept

2.2 Infrastructure Component. The part that connects the logical sides of client and server-farm is the infrastructure side. As our architecture proposes, the infrastructure has two components: gateways, which apply packet-filtering techniques on data leaving or arriving at the client side or the server-farm side, and the logical path between sites. The infrastructure component ensures security of data passing through the institutions' backbone or through the Internet from site to site (Cisco, 2010). The gateway, located at the edge of each site, is designed to block unauthorized access while permitting outbound communication.

2.3 Client Component. The user's interaction with the authentication system is represented by an eToken smartcard. By using this solution we ensure the transparency of the security methods and user mobility, thus enabling a doctor to access a certain patient chart from any end-terminal in the network. The user's authentication in the system is done by entering the smartcard's PIN. Based on the rights of the user's Organizational Unit the interaction with the database is limited by the rank of the user in the institution. Relative to the medical specific legislation we defined several groups of users: administration personnel, head of department, doctors and nurses. Each of these groups are limited to their own department and based on their rank.

Computers installed in medical offices are considered end-user systems (Alexandru *et al*, 2010). At each terminal is connected a SmartCard reader (Fig. 2), that if a smartcard is inserted, authentication is done and the access of the terminal to hospital servers is opened. The doctor session can be opened/created only using the doctor's SmartCard. When this smartcard is inserted into the reader a secure communication channel is created between the host application and smartcard. After mutual authentication the physician's PIN number is required to be entered.

The smartcard validates the entered PIN, and then opens a communication session and the host application can communicate with remote hospital server. The hospital server's network address is obtained from the smartcard. Doctor's personal information and private key DSA (Digital Signature Algorithm) are temporarily sent to the host application, and they will be deleted when the session is closed. After the doctor's session opens, the host application waits for patient's smartcards to occur, to create/open sessions of the patient.

When a doctor session is opened, the host application can accept the patient's smartcards to open sessions of the patients. For this, to the medical office computer must be connected a second smartcard reader. As for the doctor's session a secure channel is created and mutual authentication is performed between the patient's smartcard and the host application.

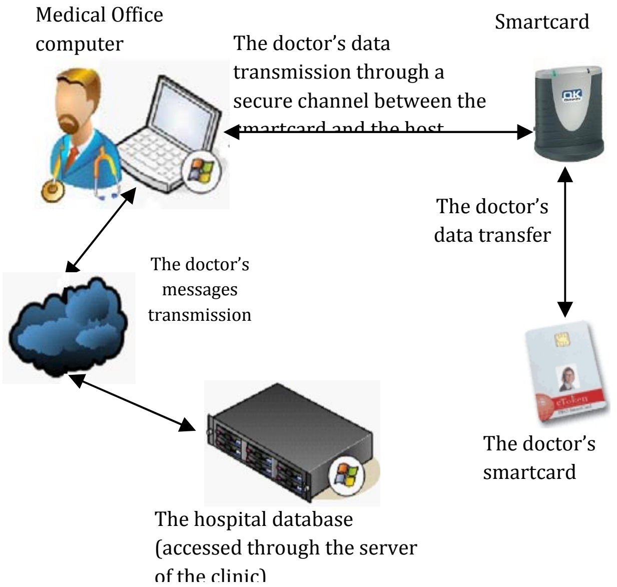

Medical Office computer
The doctor's data transmission through a secure channel between the smartcard and the host
Smartcard
The doctor's data transfer
The doctor's messages transmission
The doctor's smartcard
The hospital database (accessed through the server of the clinic)

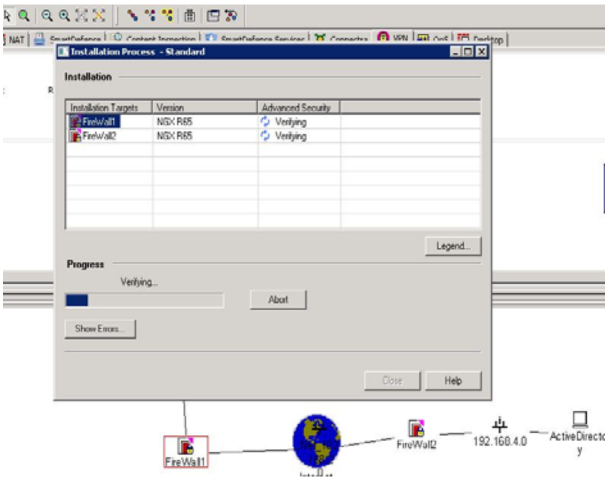
Fig. 2 The smartcard session for the doctor's access

After verifying the entered PIN, the patient data is transferred from the smartcard to the host application. To obtain the patient's health data, a secure communication channel with the hospital server is created. The terminal computer receives data requested from the server in encrypted form. The data is encrypted and decrypted using the DES (Digital Encryption Standard) key stored in the patient's smartcard.

3. SIMULATION MODEL

To create VPN community is necessary to specify a name, establishing a security policy for domestic traffic of the community, adding the participating gateways, VPN tunnel properties and other advanced settings.

The last step in configuring the environment is to install VPN policies, installation taking place all through the interface provided by SmartDashboard. Figure 3 shows the installation progress of those policies on the two gateways involved in the VPN community, suggestively named FW1 and FW2.


Installation Process - Standard

Installation

Installation Targets	Version	Advanced Security
FireWall1	NGX R65	Verifying
FireWall2	NGX R65	Verifying

Progress

Verifying...

Fig. 3 Installing VPN policies

To verify the correct routing of packets and VPN tunnel operation were carried out a series of tests based on the VPN protocol, which covered all possibilities of interaction between virtual environment entities and the host server of the virtual machines. The most complex of the tests verified the possibility of communication between the extremities of architecture: the instance for network entities management, SmartCenter and the ActiveDirectory server; the communication involves also configured firewalls that serve as gateways to a public data network. As mentioned in the paper introduction, the simulation environment used to evaluate the architecture is Opnet. Both behavior and performance of modeled systems can be analyzed by performing discrete event simulations.

3.1 Topology. The designed topology illustrates the proposed architecture, consisting of the three logical layers. Each logical subnet consists of 50 client workstations interconnected by an OSI layer 2 switch. In order to interconnect the client networks with the server farm, an Unsecured Packet Data Network (PDN) is simulated, representing the Internet. In order to connect securely to this network, each client LAN has a Gateway. Each client Gateway controls the traffic as well as the security policies specific to the proposed architecture.

The Server Farm component accommodates the entities that provide all services for the clients. The core component, of this logical unit, is the database server. Auxiliary functions, such as secure remote login, must be provided. Also a Gateway is used in order to provide the necessary security and traffic engineering requirements. In order to run the simulation, Opnet requires two auxiliary configuration units: Application Config and Profile Config. These modules provide the necessary parameters for the Discrete Event Simulation (DES), Fig. 4.

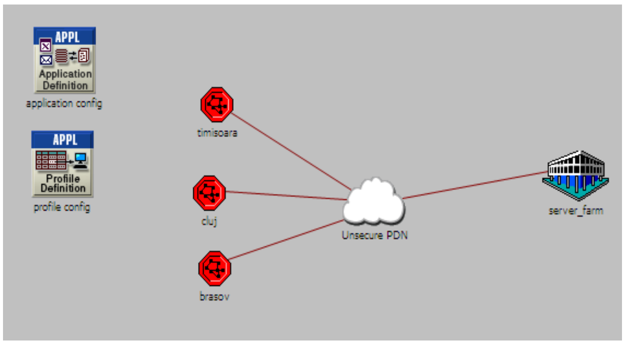


Fig. 4 Basic network simulation model

Because this architecture is primarily targeted towards healthcare facilities, we can safely assume that the main traffic model consists of heavy database usage and light remote login. To reflect this, we configured the appropriate applications and profiles. Given the fact that scalability is one of the key features of the architecture, two scenarios were created, in order to assess the behavior of the server farm under light and heavy client load. Thus, in the base scenario, the client level consists of 150 hosts, grouped in three logical subnets, each representing one county hospital. In the second scenario, we extended the client level to accommodate 2000 client workstations grouped in 40 county hospitals.

3.2 Discrete Event Simulation. The basic concept of the Discrete Event Simulation is that state variables change at discrete points in time. This approach is the most efficient in studying packet data networks. The simulation focuses on two key characteristics of the proposed architecture: scalability and data security. First of all scalability is clearly demonstrated by increasing the clients count, thus generating more throughput in the network. The main network characteristics that were analyzed are global Ethernet delay, link utilization and server characteristics such as task processing time, traffic received and traffic sent.

To underline the differences between the two variations of the scalability scenario, relative to the analyzed characteristics, statistical data was gathered while running the simulations simultaneously. To obtain a clear perspective the results were overlaid in the following graphs.

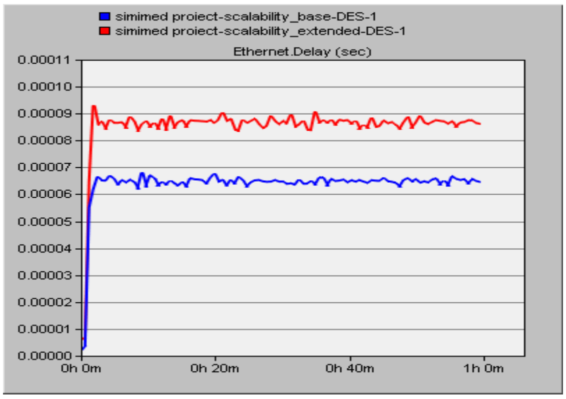


Fig. 5 Global Ethernet Delay

In the Fig. 5 the global Ethernet delay is shown, the red line (up) represents the larger network (2000 clients) and the blue one represents the reference network (150 clients). As expected the overall delay increases, but only by approximately 25% while the client number is increased almost 10 times. The uplink from the server farm to the public data network is critical because if it becomes congested it can act like a bottleneck for the entire architecture. As presented in Fig. 6 link utilization increases 8 times, directly proportional to the client increase. To avoid congestion scenarios, multiple and redundant uplinks must be provided at the server farm site.

The final statistics that were gathered refer to traffic sent/received to/from the database server (Fig. 7 and Fig. 8). As expected both traffic types show a significant increase from one scenario to another. These results show a more detailed view of the inbound/outbound traffic, and its effect on server load.

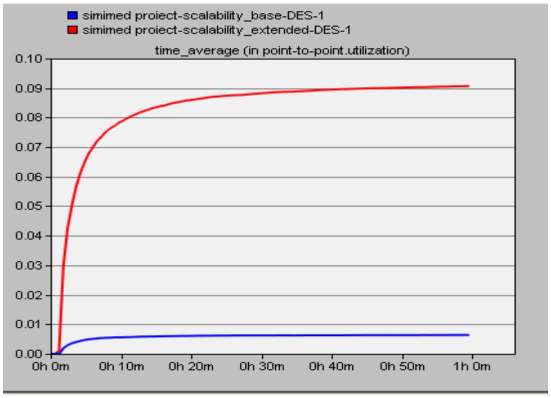


Fig. 6 Server Farm Uplink Utilization

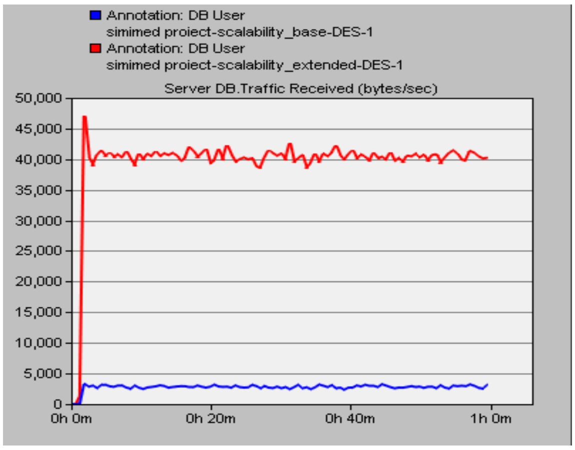


Fig. 7 Traffic received by database server

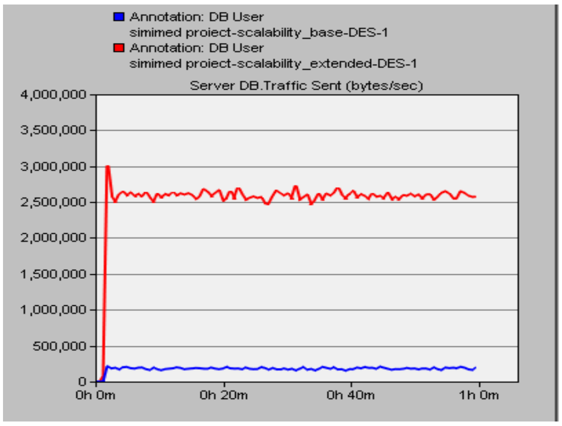


Fig. 8 Traffic sent by database server

These two statistics show an important characteristic of database scalability. While the number of requests increases dramatically, the traffic toward the client workstations has a slightly lower increase rate, which shows the server's ability to scale under high demand.

To complete the simulation of the proposed topology, a layer of security was added: VPN. In order to integrate the VPN layer into the simulation, a new scenario was created, in which tunnels between each border gateway were configured and an IP VPN configuration entity was added.

Fig. 9 presents the differences between the scenarios after the simulations were rebuild and the results were overlaid. The red line represents global Ethernet delay for the unsecure scenario, while the blue line (up) the secure scenario.

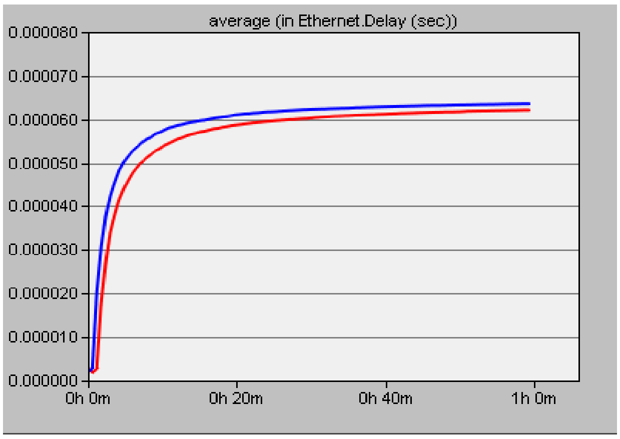


Fig. 9 Ethernet delay differences

4. CONCLUSIONS & ACKNOWLEDGMENT

This paper is a study on implementing a smartcard-based HIS system, built on a three-tier software architecture, which contains levels of client, server and database, placing also the problem of secure connections between them.

Considering the scale of the proposed architecture, number of users and traffic generated trough out the entire network, it is impossible to correctly say how traffic flows and site configuration might affect network performances. Thus it is imperative to run a complete set of simulations.

After designing the layered topology and mirroring it into the software, we ran a series of simulations in key nodes throughout the network, while also considering global statistics such as global Ethernet delay. There were created two scenarios in order to highlight the topology's scalability and secure data communications throughout the architecture.

It was demonstrated that in a controlled simulation environment the differences in global Ethernet delay between the two scenarios are relatively small, considering the advantages that VPN tunnels offer.

BIBLIOGRAPHY

1. Alexandru, M., Toev, R., Scutaru M. (2010). Study on Secure Networks' Scalability in Healthcare Facilities, Cluj Napoca: *IEEE International Conference on AQTR*, pp. 239-242.
2. Cordos, A., (2008). Studies and research on the management, processing and transmission of healthcare information, *Doctoral thesis*, Technical University of Cluj-Napoca.
3. Scutaru, M., Ţoev, R., Romanca, M., Alexandru, M. (2009). A New Approach for a Healthcare Network Architecture and Security, Athens: *Proceedings of the WSEAS International Conferences (ACC'09)*, Vol. II, pp. 557-562.
4. Tan, J., Wen, H., Gyires, T. (2003). M-commerce security: The impact of wireless application protocol security services on e-business and e-health solutions, *International Journal of M-Commerce*, Issue 1(4).
5. Xudong, L., Huilong, D., Haomin, L., Chenhui, Z., Jiye, A. (2005). The Architecture of Enterprise Hospital Information System, *Engineering in Medicine and Biology Society*, pp. 6957-6960.
6. *** (2010). White paper: Cisco Unified Communications and Service-Oriented Network Architecture. Available [2010]: http://www.cisco.com/en/US/solutions [20 may 2010].