Computer Science Journal of Moldova, vol.**16**, no.3(48), 2008

Confidentiality and Security in Medical Information Systems

Victor Papanaga

Abstract

Behind the technologies Medical System contains different types of information including patient information also. The patient data is classified as confidential and is one of the patient rights based on World Health Organization declaration. There are several compromises in solutions selection based on hardware and software requirements, performance, usability, portability. This article presents the investigation results and proposes the secured solution principles for the medical system that deal with patient data.

Keywords: Medical Information System, World Health Organization, Patient Rights, Patient Confidentiality, Patient Data, Medical Investigations Data, Medical Security, Symmetric/Asymmetric Encryption, Encryption Key

1 Introduction

Medical Information Systems (MIS) in majority cases deal with patient information. According to World Health Organization (WHO), coordinating authority for public health, patient rights include:

- The right to receive information from physicians and to discuss the benefits, risks, and costs of appropriate treatment alternatives;

- The right to make decisions regarding the health care that is recommended by the physician;

- The right to courtesy, respect, dignity, responsiveness, and timely attention to health needs;
- The right to confidentiality;
- The right to continuity of health care;
- The basic right to have adequate health care.

In most of the cases physicians assure that patient rights are not compromised but with implementation of the MIS the responsibility to assure the confidentiality of the patient information becomes the actual problem for Software Engineers that create and implement MIS. In this situation the accuracy in selecting the solution that assures the patient confidentiality becomes vital for the project implementation. This article presents the investigation results for Secure MIS implementation based on the most common hardware and software constraints.

2 Patient information in Medical Information Systems

Behind the pure medical information like Medical Knowledge Databases, present medical systems usually deal with additional information like user database, patient database, medical investigation database, other. In situation when the database contains patient information, the system must assure the confidential access to such information.

Minimal patient information usually available in Medical Systems is:

a. **Patient data.** Minimal data to identify the patient are: **Name**, **Surname** but there are some constraints that require additional information as following:

    - Using **Name** and **Surname** there are some risks to identify ununiquely the patient. For unique identification we

  will require additional information like **Unique Identification Number** (IDNP) allocated for each citizen on birth. **IDNP** is required also in registration of the patient visits to physicians provided by Healthcare Institution to Medical Assurance Institutions.
  - To differentiate physiological aspects for male and female anatomy the systems can add additional description for patient like **Sex**.
  - Differences based on patient age can be monitored using additional descriptor like **birth date**.

b. **Patient investigation data.** Patient investigation data include the following:
  - Information about fact of addressing for medical help;
  - Present health situation;
  - Diagnostic Disease;
  - Other medical data collected after additional investigation.

Sometimes when the medical data are collected using specialized devices the patient information is included in digital collected information (example of ultrasound investigations as images, movies contains patient information), that's why the confidentiality of the patient data requires additional attention to digital resources also.

Based on World Health Organization, all the **Patient investigation data** are classified as confidential and require attention in elaboration and implementation of MIS.

There are several international standards elaborated by specialized institution that describe and offer the recommendations in implementation of the security components in MIS like:

- ISO TC 215 (ISO)
- HL7 (Health Level Seven)

- CIHI (Canada)
- GEHR
- ICPC (EUPHID)
- SONOMED
- Current Procedural Terminology
- OPCS-4, UT
- DICOM
- XML (W3C Consortum)

Chosen solution requires conformance with existing standards and deep attention in application implementation.

3 Constraints in provided solutions

There are a lot of existing solutions that assure the encryption of the textual, digital and media, stream information. Several solutions are pure hardware, other are software or combined. Based on application type the solutions can be: free or priced, open source or custom, platform independent or based on specific platform. In our case there are several constraints that require attention in solution providing/implementation as following:

- **Easy system integration** – solution requires to be integrated or part of the main system;
- **Short processing time** – solution that performs the action fast;
- **Independent solution** – solution that does not require human interaction directly;
- **Platform Independent** – solution that easy can be used and/or adjusted for each type of OS platform;

- **With low implementation cost** – solution that does not require additional costs for hardware upgrades, software license, other.
- **With minimal resources usage** – solution that supports minimal hardware configuration for the system and does not affect the performance.
- **Solution that allows textual and digital information encryption / decryption**.
- **Solution that allows integration with third part components** (like database readers/writers)**.**
- **Solution with easy further maintenance.**

4 Available software to satisfy the selection criteria

In order to find the possible third part solution to satisfy our application the set of the Internet Available applications were investigated and the results of investigation are presented in Table 1.

General comments related to preliminary investigation:

- There is no free or non free software that satisfies all mentioned criteria for Medical Systems;
- All the existing solution are classified as final products and can't be integrated using API or other technologies to our system;
- All the identified solutions are platform dependent and based on Windows OS predominantly;
- There is no free (only shareware) solution to satisfy our necessity;
- All the identified solutions are easy to maintain based on specialized interface but not assure the integration with third part components.
- We can obtain some progress in this direction only if we will develop our custom solution.

Table 1. Encryption/Decryption software acceptance criteria conformance

Application	Easy system integration	The short processing time	Independent solution	Platform Independent	With low implementation cost	With minimal resources usage	Solution that allow textual and digital information encryption /decryption	Solution that allow integration with third part components	Solution with easy further maintenance.
File Encryption XP 1.5.123		■				■	■		■
Best Folder Encryptor 15.72		■					■		■
BestCrypt Volume Encryption 2.11.01		■					■		■
Max File Encryption 1.8		■					■		■
SecureIT Encryption Software 3.1.8		■				■	■		■
Encryption And Decryption Pro 1.2		■					■		■
Strong File Encryption Decryption 1.0		■					■		■
Folder Crypto Password 2.0		■					■		■
Dekart Secrets Keeper 3.11		■				■	■		■

Legend:

	The selected criteria are not satisfied
■	The selected criteria are satisfied

5 Cryptographic solution investigation for MIS

To satisfy all our requirements it is proposed to develop custom solution for our application. The investigation process includes two steps:

- **Step 1** – identification of the encryption methodologies (symmetric, asymmetric);

- **Step 2** – identification of the encryption algorithm

There are some constraints related to asymmetric key encryption related to public authority that must be involved in the process of key emission like VeriSign, other. Asymmetric key also has it own life cycle and needs to be re-emitted periodically (once a year). That's why it compromises one of our criteria: **Solution with easy further maintenance.** At the same time we can't decide to exclude it from our performance investigation that's why the most representative asymmetric algorithm was selected for performance compare.

Step 1 – the investigations main purpose was the identification of encryption methodologies.

Exercise was done using IntelliJ Idea 7.3 on Windows Vista with 2 GB RAM and 100 GB hard disk for 10 times and average results are presented in Table 2.

Note: This test includes run-time symmetric key generation, encryption of plain text into cipher text and decryption of cipher text back into plain text.

Summary of observations:

- Regardless of the algorithm (and therefore the perceived complexity of the algorithm) the amount of time it takes for encryption and decryption remains more or less the same.
- The size of the input text does not make any difference.

Note: This test includes run-time symmetric key generation, encryption of plain text into cipher text and decryption of cipher text back into plain text. Asymmetric key algorithm performance is presented in Table 3.

Summary of observations:

- The time taken is certainly more than what symmetric key encryption algorithms require.

Table 2. Symmetric algorithm encryption/decryption performance

Algorithm used	**Original text**	**Length of original text (kb)**	**Key size (bit)**	**Execution time (ms)**
Blowfish	Small plain text for encryption	32	128	40.0159098
	Medium plain text for encryption	85	128	41.2025411
	Big plain text for encryption	203	128	40.0815467
3DES	Small plain text for encryption	32	160	41.5861513
	Medium plain text for encryption	85	160	40.5570750
	Big plain text for encryption	203	160	41.3329487
AES	Small plain text for encryption	32	256	42.7647718
	Medium plain text for encryption	85	160	42.3849121
	Big plain text for encryption	203	160	42.4304486

- The size of the input text is important. The more the plain text, the higher is the time taken for encryption and decryption.

Conclusion:

- To assure performance in Medical Information Systems the Symmetric Key Algorithms are preferable and provide the best performance as Cryptography methodology;

- Not all symmetric cryptographic solutions are approved by international standards (from our list only 3DES and AES satisfy this criteria).

Table 3. Asymmetric algorithm encryption/decryption performance

Algorithm used	**Original text**	**Length of original text (kb)**	**Key size (bit)**	**Execution time (ms)**
RSA	Small plain text for encryption	32	1024	86.1157563
	Medium plain text for encryption	85		88.0750277
	Big plain text for encryption	104		93.0025534

Step 2 – the investigations main purpose was the identification of encryption algorithm and minimal hardware environment for Encryption process.

Exercise was done using JDK 1.4.2 and JDK 1.5.13 on Pentium IV 2.4 GHz with 256 Mb RAM, running Windows XP Professional edition. Exercise was performed for 10 times and average results in **milliseconds** are presented in the Table 4.

Summary of observations:

- Observation was performed using minimal hardware environment for Pentium IV technologies;
- Observation includes encrypt and decrypt process;
- For low and medium block size, AES algorithm performs encryption and decryption much faster;
- For increased block size the algorithms have the temptations to provide the same results;
- AES algorithm is acceptable as Encryption Algorithm by international standards;
- AES algorithm has the public implementation and can be developed in platform independent mode using Java technologies.

Table 4. 3Des and AES encryption/decryption performance

Block Size		**Java SDK**			
		Java 1.4.2		**Java 1.5.13**	
		Encrypt	**decrypt**	**encrypt**	**Decrypt**
1Kb	**3DES**	0	0	0	0
	AES	0	0	0	0
10Kb	**3DES**	0	0	0	0
	AES	0	0	0	0
100Kb	**3DES**	31	31	15	31
	AES	0	0	0	16
1Mb	**3DES**	328	360	343	375
	AES	94	109	109	141
10Mb	**3DES**	2860	2891	2859	2958
	AES	500	547	500	562
50Mb	**3DES**	16063	14948	14703	16373
	AES	4641	4250	2328	4875
100Mb	**3DES**	116687	124969	78765	110828
	AES	98094	103813	66531	74375

6 Conformance with initial selection criteria

Utilization of the Java based solution for our algorithm satisfies the initial selection criteria as following:

- **Easy system integration** – utilization of the universal solution (Example: based on Java);
- **The short processing time** – the processing time is shorter than other concurrent solutions;
- **Independent solution** – solution can be developed in such a way that to exclude human interventions;
- **Platform Independent** – utilization of Java Based solutions for algorithm;
- **With low implementation cost** – utilization of existing open source solutions for algorithm;

- **With minimal resources usage** – algorithm is faster than several concurrent solutions. Additional constraint was added in order to satisfy WHO and international standards requirements;

- **Solution that allows textual and digital information encryption / decryption** – was demonstrated under test process;

- **Solution that allows integration with third part components** – as custom solution there are possibilities to create the Public API in order to integrate to third part components.

- **Solution with easy further maintenance** – there are no any constraints in symmetric key lifecycle and the maintenance of the key can be properly organized and/or documented.

7 Conclusions

- There is no public free solution to satisfy Medical Information System requirements in cryptography implementation;

- Symmetric algorithms are faster than asymmetric algorithms and can be used in simple Medical Information System with low resource limitation;

- AES is faster than 3DES algorithm for small and medium block size. For block size more than 100Mb the performance is comparable with 3DES algorithm;

- AES algorithm satisfies the initial selection criteria and can be used as possible solution for Medical Information Systems.

References

[1] Bert JAGERS. *Comparing file transfer and encryption performance of Java and .NET.* Academiejaar 2003 – 2004;

[2] Gregory L. Orgill. *JAVA PERFORMANCE OF THE RIJNDAEL ENCRYPTION ALGORITHM ACROSS COMPILERS AND VIRTUAL MACHINES.* Brigham Young University Publishing, April 2005;

[3] P. Y.A. Ryan, S. A. Schneider. *The Modelling and Analysis of Security Protocols: the CSP Approach.* Addison Wesley, December'2000;

[4] Michael Cross. *Development Guide to Web Application Security.* Syngress Publishing, Inc., 2007;

[5] Jonathan B. Knudsen. *Java Cryptography.* O'Reilly, 1998.

Victor Papanaga,

Received November 10, 2008

Institute of Mathematics and Computer Science of Academy of
Science of Moldova
Str. Academiei 5, Chişinău, MD-2028, Moldova
Phone: (+ 373 22) 56 87 43
E–mail: *vic_papanaga@yahoo.com*