32

Security Enforcement in a European Medical Device Vigilance System Network

G. Vassilacopoulos, V. Chrissikopoulos and D. Peppes

Department of Informatics, University of Piraeus,
80 Karaoli & Dimitriou Str. 185 34 Piraeus, Greece
tel. : +30 1 4222124
fax : +30 1 4179064
e-mail : gvass@unipi.gr , chris@unipi.gr and pepes@unipi.gr

Abstract

The medical device vigilance system (MDVS) is a Europe-wide system concerned with the exchange of information, generated from the process of investigating a medical device incident, among various authorized parties. Due to the sensitivity of the exchanged information, security is of primary importance. In order to address the security requirements of the MDVS, a communication protocol is proposed that is provably secure and practical for implementation. In addition, a scenario for the operation of the MDVS network based on this protocol is presented.

Keywords

Network security, communication protocols, health telematics

1 INTRODUCTION

The Medical Device Vigilance System (MDVS) is a Europe-wide system that has been created in response to the requirements imposed by the AIMD and MD directives of the European Union (EU) on medical devices (Council Directive 1990, Council Directive 1993, Commission 1993). The system has three main objectives: (i) the protection of reoccurrence of incidents with the same type of medical device, at another place, at another time; (ii) the encouragement of manufacturers to perform investigations and take corrective actions if necessary; and (iii) to enable competent authorities to monitor the investigation procedures and intervene when necessary.

S. K. Katsikas et al. (eds.), *Information Systems Security*

To achieve these objectives, a large amount of data needs be stored and communicated among the parties involved in the investigation and reporting process regarding a medical device incident. This need gave rise to the European Medical Device Information Exchange System (EUROMEDIES) concerted action project (EUROMEDIES 1995). The main objective of this project is to specify the requirements for a telematics-based system with respect both to database applications for storing regulatory data and incident reports, pertaining to medical devices, and to network services provided for the exchange of this information between the parties involved in an incident investigation and reporting process.

Due to the sensitivity of the data related to medical device incidents, especially before a final conclusion is reached, information security has been one of the main concerns of the project. Thus, appropriate security mechanisms should be identified in order to maintain the confidentiality and integrity of sensitive data by taking into account factors such as usability, performance and cost. Although this involves both database and network security, this paper focuses on the latter. Specifically, we propose a network security protocol that is able to address adequately the network security requirements regarding the exchange of information within the MDVS.

2 THE MDVS COMMUNICATION REQUIREMENTS

The parties involved in a medical device incident investigation and reporting process within the MDVS are: competent authorities (e.g. Ministries of Health), notified bodies (e.g. standardization organisations), manufacturers and/or their authorised repre-sentatives, users of the medical devices (e.g. hospitals) and the Commission of the EU.

On reporting an incident related to a medical device, a number of actions are taken within MDVS concerning the incident's investigation. Among these are included:

- A first evaluation of the conditions under which the device was involved in the incident.
- An initial report (within 10 or 30 days) from the manufacturer to the competent authority proposing either to close the case or to investigate it further.
- Intermediate communication among parties concerning the type of medical device involved in the incident.
- An in depth investigation carried out by the manufacturer under the control of the responsible competent authority.
- A final report proposing actions to be taken or not.
- Transfer of information to the other competent authorities or other involved parties and the Commission of the EU on the results of the investigation and, possibly, on measures to be taken.

Thus, within the context of the medical device vigilance procedures there is a frequent flow of information among the various parties involved in an incident investigation process. In particular, the exchange of information among parties becomes necessary when measures have to be taken, or envisaged, as a consequence of an incident report. For example, data

related to the final report on the investigations regarding the incident should be made available to all competent authorities, while those related to the previous phases of the process should be made available on request. Figure 1 shows a simplified view of the communication among the various parties involved in investigation and reporting process regarding a medical device incident.

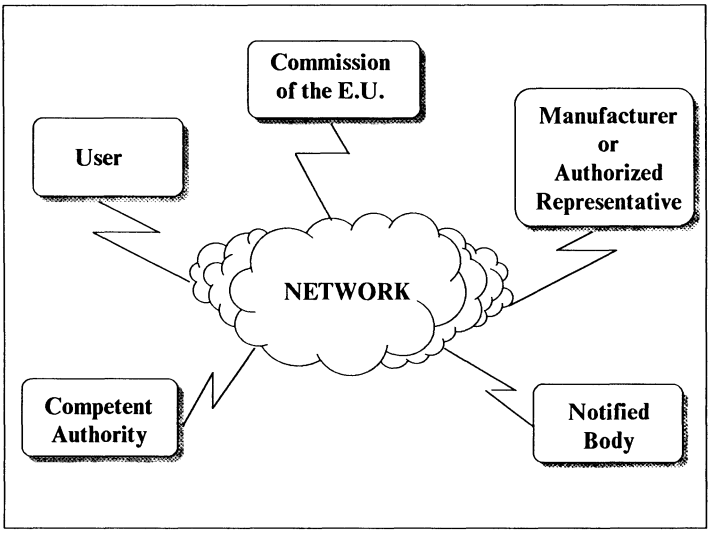

Figure 1 A simplified view of communications within MDVS.

During information exchange regarding an incident there is a need to ensure that relevant information is accessible only by authorised parties since, otherwise, the reputation of the particular medical device can be put at stake. Therefore, any network established with the objective to facilitate information exchange within MDVS should be tightly protected. However, the level of security that should be included in the system involves some judgement about the dangers associated with the system and the resource implications of various means of avoiding or minimising those dangers (EEC/DGXII 1991). Risk analysis issues have been considered within the framework of the EUROMEDIES project in collaboration with representatives of the involved parties (especially manufacturer associations).

3 AN MDVS NETWORK SECURITY PROTOCOL

Network security is usually provided through encryption/decryption of the exchanged information (EEC/DGXII 1991, Pfitzmann-Pfitzmann 1991). Security in the MDVS network is required to ensure that medical device incident information exchanged among various

parties is protected from such threats as message injection, message reception by unauthorised receivers and transmission disruption (EUROMEDIES 1995).

In general, the services that a network security system should provide are (ISO/IEC 1989, EEC/DGXII 1991, Pfitzmann-Pfitzmann 1991, Janson-Molva 1991): entity authentication, data confidentiality, data integrity and non-repudiation. In addition to these services, the MDVS network requirements call for the simultaneous participation in a communication by two or more parties. For example, when a medical device incident occurs, the user where the incident occurred, the competent authority of the country of incident and the manufacturer (or authorized representative) of the medical device involved may begin a communication session regarding the incident. In addition, the notified body that has provided certification for the medical device can take part in the communication session.

In order to provide these services, a secure communication protocol is required. Although a number of communication protocols, where the involved parties are more than two, have been proposed, most of these are either impractical for implementation or based on heuristic arguments to address their security (Ingemarsson et al. 1982, Koyama-Ohta 1988, Tsujii-Itoh 1989, Fischer-Wright 1992, Blundo et al. 1993). The protocol proposed in this paper is provably secure and relatively easy to implement due to its low communication and low computational complexity (Chrissikopoulos-Peppes 1995). This protocol is based on the intractability of the Diffie-Hellman problem (Diffie-Hellman 1976) and extends the features provided by the protocols proposed in (Matsumoto et al. 1986, Yacobi 1991, Burmester-Desmedt 1995).

According to the proposed protocol, a Trusted Centre chooses the security parameters (p, α and q, where p is a prime number , $\alpha \in Z_p$ whose order q is a large - superpolynomial in $|p|$). These parameters are announced to the parties registered as network users.

Let N be the number of parties registered as network users and $U_1, U_2, \ldots, U_n$ ($n \leq N$) be a set of parties that want to generate a common shared key in order to have a secure conference (the value of n may vary between conferences but it needs to be fixed for each conference).

In the first phase of the protocol, each party U_i selects a secret key s_i and registers with the Trusted Centre the value

$$P_i = a^{s_i} \bmod p$$

as its public key. In the second phase, each party selects a random number r_i from the set Z_p, computes a value

$$X_i = a^{r_i} \bmod p$$

and sends this value to the other parties in the conference. Then, each party is taken in a cycle and computes a value

$$Y_i \equiv (P_{i+1})^{r_i} / (X_{i-1})^{s_i} \equiv (X_i)^{s_{i+1}} / (P_i)^{r_{i-1}} (\bmod p)$$

which is also sent to the other parties in the conference. The common shared key is computed by a combination of all 5-tuples $(P_i, X_i, Y_i, r_i, s_i)$ as

$$K \equiv a^{r_1 s_2 + r_2 s_3 + \ldots + r_n s_1} (\text{mod } p) .$$

This key can be computed by every party U_i in the conference since

$$K \equiv K_i \equiv (X_{i-1})^{n s_i} . Y_i^{n-1} . Y_{i+1}^{n-2} \ldots Y_{i-2} (\text{mod } p) .$$

Figure 2 shows the conference key distribution system for three communicating parties.

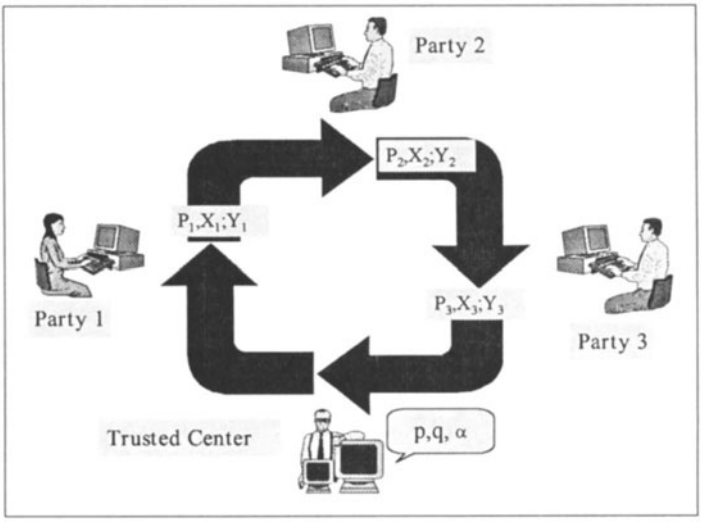

Figure 2 The conference key distribution system for three parties.

The described procedure needs to be executed each time two or more parties want to start a secure communication. When the parties have in their possession this common shared key, they can use any encryption algorithm to encrypt/decrypt the sensitive information transmitted over a public and insecure channel. For example, a DES-like algorithm can be used (US 1977).

In the above procedure, the role of the Trusted Centre is restricted to the selection of the appropriate parameters and to the management of the network security system. Thus, the common shared key is derived by the parties in such a way that no party can predetermine this key. After the execution of this protocol only an authenticated party can be in possession of the correct key (or in possession of the necessary information to compute the correct key).

The above described protocol was proposed within the EUROMEDIES project on the basis of a thorough evaluation of similar purpose protocols that have been presented in the literature (Koyama-Ohta 1988, Okamoto-Tanaka 1989, Tsujii-Itoh 1989, Chrissikopoulos-Peppes 1995). The results of the evaluation process are summarized in Table 1. The Ingermarsson, Tang and Wong protocol (Ingemarsson et al. 1982) and the Burmester and Desmedt protocol (Burmester-Desmedt 1995) are not included in Table 1 because they have similar characteristics to the one presented here. However, the former is not provably secure.

Table 1 A comparison of the characteristics of various protocols

Protocols	*Koyama Ohta*			*Tsujii Itoh*	*Okamoto Tanaka*	*Chrissikopoulos Peppes*
Characteristics	1	2	3			
The Trusted Centre knows the secret keys	Yes			Yes	Yes	No
User Computations (for m users)	11 exps	8m+1 exps	8m+1 exps	2 exps	2 exps	4m exps
Total number of rounds	m-1	3	3	1	1	3
Total Number of exchanged messages	m(m-1)	3m(m-1)	3(m-1)	---	1	2m
Freshness of session keys	Yes			No	Yes	Yes
The Security is based on	Factoring large numbers and the Discrete Logarithm (DL) problem			DL problem	Diffie Hellman problem and RSA	Diffie Hellman problem

4 IMPLEMENTATION

On the basis of the security protocol described above, a scheme for a secure network system can be established. To this end, there is a need to select an organization that will play the role of the Trusted Centre (e.g. the Commission of the EU) and to develop the necessary applications for the enforcement of the protocol into the network. Then, an operational scenario of the system could be as follows:

- Parameter Selection. The Trusted Centre defined lays down all the system parameters.
- Party Registration. A party (user, competent authority, manufacturer or notified body) that wishes to become a network user will have to apply to the Trusted Centre for authorization. After its acceptance, the party selects a secret key and computes its public key which it registers with the Trusted Centre. This public key has to be distributed to all authorized parties or to be stored into a central database (held at the Trusted Centre) accessible by all the authorized parties. In either case, the authorized parties have only read access to the database of the public keys.

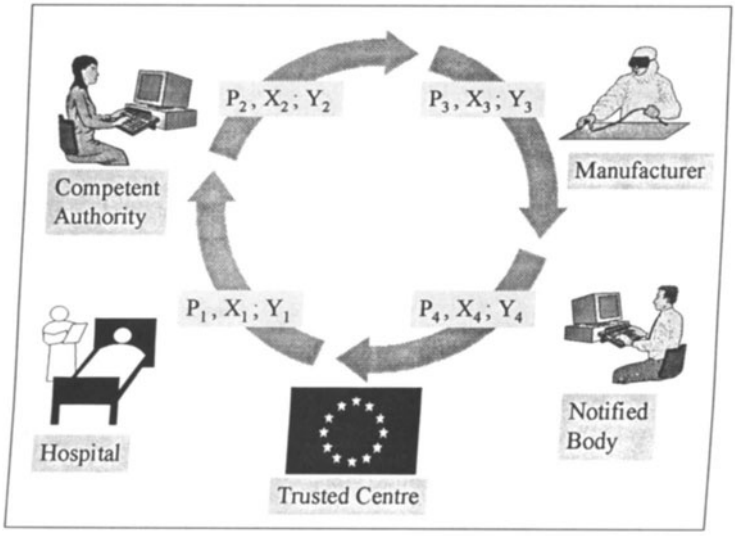

Figure 3 A secure conference within the MDVS.

- Secure Conference. When a medical device incident occurs, the relevant user informs its competent authority through a national reporting system. In turn, the manufacturer is informed by the competent authority and the relevant notified body may be called in the conference. At this stage the conference can begin and the procedure described earlier is executed in order to specify a common shared key among the participants. This key is used

to encrypt/decrypt the information exchanged among parties and to ensure a secure conference. Figure 3 shows a view of a secure conference among four parties within the MDVS (it is assumed that after computing the common shared key, the conference participants communicate through the MDVS network).

Within EUROMEDIES, a proposal has been put forward to use an Electronic Data Interchange (EDI) network for the exchange of information within the MDVS [EUROMEDIES 1995, Pramataris et al. 1995]. An EDI communication is based on predefined formats of the information that is transmitted among the parties involved, even if these parties use different applications. Since the proposed protocol is independent of the format used to exchange information, it can also be used in conjunction with an EDI network. The need for security in EDI based communication systems is described in [Williamson-Draper 1991, Olnes 1993].

5 CONCLUDING REMARKS

A provably secure communication protocol for information exchange within the MDVS is proposed. The protocol is based on the intractability of the Diffie-Hellman problem and is practical for implementation due to its a low communication and low computational complexity. It ensures that the parties involved in the investigation and reporting process related to a medical device incident can communicate securely since an unauthorized party cannot be in possession of the common shared key (or in possession of the necessary information to compute this key) which the authorized parties use to encrypt and decrypt their exchanged information.

6 REFERENCES

Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M. (1993) Perfectly-secure key distribution for dynamic conferences. *Advances in Cryptology-Crypto' 92, Lecture Notes in Computer Science #740,* (ed. E. Brickell), Springer-Verlag, 471-487.

Burmester, M. and Desmedt, Y. (1995) A Secure and Efficient Conference Key Distribution System. *Advances in Cryptology-Eurocrypt' 94,* (ed. A. De Santis), Springer-Verlag, 275-286.

Chrissikopoulos, V. and Peppes, D. (1995) A Practical Conference Key Distribution System. *Information Security - the Next Decade, Proceedings of IFIP/SEC'95, The 11th Inter. Information Security Conf.,* (eds. J. Eloff and S. Solms), 168-175.

Commission of the European Communities (1993) *Guidelines on a Medical Devices Vigilance System.*, Directorate-General, Industry, Brussels.

Council Directive 90/385/EEC. (1990) Official Journal of the European Communities L 189.

Council Directive 93/42/EEC. (1993) Official Journal of the European Communities L 169, **36**.

Diffie, W. and Hellman, M. (1976) New directions in cryptography. *IEEE Trans. Inform. Theory*, **IT-22**, 644-654.

EEC/DGXII, (1991) *Data Protection and Confidentiality in health informatics*, IOS press.

EUROMEDIES (EUROpean MEdical Device Information Exchange System) (1995) concerted action. Project number A2122. AIM Programme Intermediate report.

Fischer, M. and Wright, R. (1992) Multiparty secret key exchange using a random deal of cards. *Advances in Cryptology-Crypto' 91, Lecture Notes in Computer Science #576,* (ed. J. Feigenbaum), Springer-Verlag, 141-155.

Ingemarsson, I., Tang, D. and Wong, C. (1982) A conference key distribution system. *IEEE Trans. Inform. Theory*, **28** , 714-720.

ISO/IEC 7492-2 (1989) Information Technology - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

Janson, P. and Molva, R. (1991) Security in open networks and distributed systems, *Computer Networks and ISND Systems*, **22**, 323-346.

Koyama, K. and Ohta, K. (1988) Identity-based conference key distribution systems. *Advances in Cryptology-Crypto' 87, Lecture Notes in Computer Science #293,* (ed. C. Pomerance), Springer-Verlag, 175-185.

Matsumoto, T., Takashima, Y. and Imai, H. (1986) On Seeking Smart Public Key Distribution Systems. *The Transactions. of the IECE of Japan*, **E69** (2), 99-106.

Okamoto, E. and Tanaka, K. (1989) Key distribution system based on identification information. IEEE J. *Selected Areas Commun.*, SAC-**7**, 481-485.

Olnes, J. (1993) EDIFACT security made simple-the EDIMED approach, *Computers & Security,* **12**, 765-774.

Pfitzmann, A. and Pfitzmann, B. (1991) Security in Medical Networks. *Data protection and Confidentiality in health informatics, IOS press*, 231-248.

Pramataris, K., Giaglis, G., Papamichail, G., Doukidis, G. and Pallikarakis, N. (1995) The Potential of EDI in Health: The EUROMEDIES case, *Proceedings of Health Telematics 95* [To appear].

Tsujii, S. and Itoh, T. (1989) An ID-based cryptosystem based on the discrete logarithm. IEEE *J. Selected Areas Commun.*, SAC-**8**, 467-473.

U.S. Department of Commerce (1977), National Bureau of Standards, *Data Encryption Standard*, FIPS Publication **46**.

Williamson, J. and Draper, J. (1991) EDI Security - Today and Tomorrow. *Information Security,* (eds. D. Lindsay and W. Price), IFIP, 361-374.

Yacobi, Y. (1991) A key Distribution Paradox. *Advances in Cryptology-Crypto' 90, Lecture Notes in Computer Science #537,* (eds. A.J. Menezes and S.A. Vanstone), Springer-Verlag, 268-273.

7 BIOGRAPHIES

George Vassilacopoulos is an Associate Professor in the Department of Informatics at the University of Piraeus. He received his BSc from the University of Athens and his PhD from Royal Holloway, University of London in 1986. His research interests are in the areas of Health Information Systems, Expert Systems, Database Security and Simulation. He is a

member of the Greek Mathematical Society, Greek Computer Society and the British Computer Society.

Vassilios Chrissikopoulos is an Associate Professor in the Department of Informatics at the University of Piraeus. He received his BSc from the University of Thessaloniki and his PhD from Royal Holloway, University of London in 1983. His research interests include Expert Systems, Information Security and Cryptography. He is a member of the Greek Mathematical Society, Greek Computer Society, Operational Research Society of the UK and BCS.

Dimitrios Peppes is a PhD Student in the Department of Informatics at the University of Piraeus. He received his MSc at Queen Mary and Westfield College, University of London in 1990. His current interests are in the areas of Applied Cryptography, Network Security and Database Security. He is a member of the Greek Computer Society.