Proceedings of The 1st MEDINF International Conference on Medical Informatics & Engineering
MEDINF' 2003, October 9 - 11, 2003, Craiova, Romania,
Craiova Medicala Journal, ISSN 1454-6876, Vol. 5, Sup. 3, (2003): 349-352

Security Mechanisms For Electronic Patient Records In Mobile Intelligent Services

Kosmas KAPIS[2], Jan C.A. VAN DER LUBBE[1]
[1]*Delft University of Technology, Faculty of Electrical Engineering, Mathematics and Computer Science, P.O. Box 5031,2600 GA Delft, The Netherlands, J.C.A.vanderLubbe@EWI.TUDelft.nl*
[2]*Department of Computer Science, University of Dar es Salaam, P.O. Box 35062,Dar-es-Salaam, Tanzania, K.Kapis@EWI.TUDelft.nl, Kapis@cs.udsm.ac.tz*

Abstract. The deficiencies found in conventional paper-based patient records, practiced in healthcare service provision, have resulted in the emerging development of electronic patient record (EPR) systems. This paper proposes a cryptography-based EPR security model guaranteeing the patient's record integrity, accountability, confidentiality and patient record access consent. For this model several possible cryptographic security mechanisms are studied. The advantages and disadvantages of each scheme are considered, and based on the EPR requirements the mechanism with best results is suggested.

1. Introduction

The limitations of conventional paper-based patient records practiced in healthcare service provision have resulted in the emerging development of electronic patient record (EPR) systems. However, the main concentration of most of the EPRs has been collecting patient's records and facilitating administrative activities [5] in the respective health organizations. To date little attention has been paid to the ethical and legal issues explicated in [3,5]. Issues like the protection of privacy and security of patients (and healthcare providers) are still neglected. This is especially towards the patient record; integrity, accountability, confidentiality and record access consent issues.

This paper looks at the aforementioned EPR shortcomings and proposes a generic crypto-based security model. It focuses on the security and privacy of EPRs.

2. Cryptographic building blocks

Let *m* be any file that contains information, e.g. an EPR. In order to protect it against 'eavesdropping' by intruders or unauthorized persons, *m* can be **e**ncrypted by using a secret key *K*. The corresponding result is denoted by **e***K*(*m*)**,** i.e. the result of encryption of *m* by using *K*. Similarly, **d***K(m)* is the result of **d**ecryption with *K*.

Signatures can provide authenticity of *m* as well as of its origin. In general, in order to generate digital signatures two keys are needed; a secret key *S* and a public key *P*. The secret key *S* is used for the generation of a signature. Due to the secrecy the owner of that key is the only one that can make a valid signature. The secrecy of the key guarantees the authenticity of

the signature. The public key *P* is used for signature verification. It enables to check whether the signature is authentic and thus valid. Since everybody should be able to check the signature, the verification key *P* is public. If *m* is provided with a digital signature by using *S*, this is denoted by ***sign****S(m)*. The verification of that signature with the help of public key *P* is denoted by **ver***P(m)*. In practice, it is easy to compute the public key if the secret key is known, but on the contrary deriving the secret key from the public key is impossible. Thus, only the owner of the secret key can generate valid signatures.

The general idea behind the proposed architecture is that the patient himself is the part-owner of and jointly responsible for his own EPR. This does justice the privacy rights and nowadays emancipation of the patient. Application of both the patient's and clinician's signature guarantee the integrity and authenticity of the EPR. This cooperation expresses that both parties agree with its contents. Encryption techniques are used for providing confidentiality. By using both digital signatures and encryption techniques it is also possible to provide privacy. In principle, this encompasses all necessary security capabilities in situations where legal disputes can occur and it guarantees that the EPR can also be accessed on the need to know bases. The proposed three mechanisms differ in the sequence in which encryption and patient's and clinician's signatures are applied.

3. Forward-secure signatures

Instead of an ordinary signature a so-called 'forward-secure signature' scheme is used [1,4]. A disadvantage of ordinary digital signatures is that if the secret key of the signer is compromised – with as consequence that everybody can make a valid signature - all the signatures become useless. That does not hold for the future signatures, but also for the past signatures. By means of a forward-secure signature scheme the validity of past signatures is preserved even if the present secret keys have been compromised. The principal of a forward signature algorithm is that several messages can be signed with a signing key S_i that eventually will be revoked and replaced with S_{i+1}. The verifier is still able to verify the messages signed with S_l for $1 \leq l \leq i$ using verifying key *P*. In this way, S_i can be disclosed to third parties after usage without difficult consequences; only an update of S_i is needed.

The basis of the algorithm is the following. Considering $yx^e = 1 \pmod n$, the following holds. If e and x are known, it is easy to computer y. However, given y and e it is impossible to compute x. The reason is that taking the logarithm module n is not feasible. By relating x in some way to the secret signature generation key *S* and y to the public verification key *P*, it can easily be concluded that knowledge about the public key *P* does not reveal the secret key *S*. Thus, only the owner of the secret key can make a valid signature. Furthermore, it is clear that there are more pairs (x,e) that satisfy $yx^e = 1 \pmod n$. Therefore, it is possible having different signing keys S_i, whereas one needs just one verification key *P*. That is exactly which have been used in the forward-secure signature scheme. Details of this algorithm can be found in [1].

4. Group Signatures

With respect to the clinician's signature a group signature scheme is chosen. The advantage of a group signature is that files or records can be signed by each member of a group anonymously on behalf of that group, as such guaranteeing the privacy of the signers. This is attractive in the case of a second opinion, where the identity of the first clinician should not be revealed. Either, it prevents clinicians controlling each other's work. Only, in the case of a dispute the identity of the group member can be revealed. Another advantage of

a group signature is that it suffices to have just one group verification key instead a number of verification keys, one for each signer. This makes the scheme less complex, at least the verification procedure. In the following it is assumed that GS and GP denote the secret and public group keys, respectively.

The algorithm is based on the discrete logarithm problem. Given $y=g^x$ (modulo n), it is easy to compute y if you know g and x, but knowing y and g it is impossible to find x. Clearly, x can be related to the secret key of the signer, y to the public key for verification. The discrete logarithm problem guarantees that nobody can find x on the basis of y and that no one can make a valid signature.

In the group signature scheme there is a group manager [2]. His secret key is GS=x and his public key – which is at the same time the signature verification key – is given by GP=y. Also each member j of the group generates a pair (x_j,y_j). However, this y_j is not public, but only known to the group manager. The group manager computes $c_j = f(y_j)$, where f(.) is a specific function and gives it back to member j. This c_j together with x_j are the secret key GS_j of group member j used for signature generation: $GS_j=f(c_j,x_j)$. Signing message m can be denoted by: **sign**GS_j(m). Verification can done by means of the public group verification key: **ver**GP(m). In the case of dispute it can be proven that the group manager can compute the value c_j on the basis of the signature and his secret key GP, relate it to the signer and thus knows the identity of the signer.

As a matter of fact it is possible to combine the concepts of a forward-secure signature and a group signature to a 'forward-secure group signature'. In the following, if it is talked about the signature, the forward-secure version is meant.

5. Security solutions

Choosing for forward-secure signatures and group signatures there are three main solutions.

Figure 1. Security mechanism I

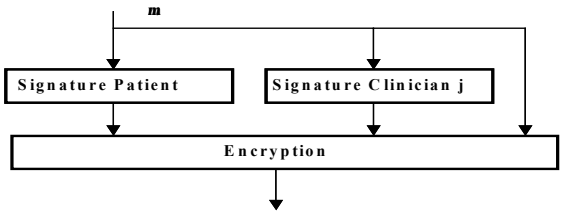
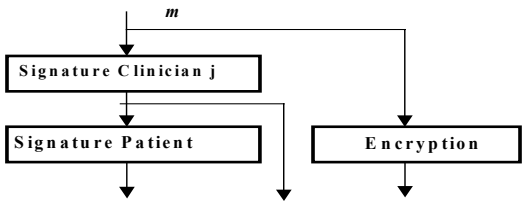


Figure 2. Security mechanism II



In mechanism I, the health care provider (HCP) e.g. clinician j, and the patient each sign on the same medical record *m*, using the group private key GS_j of the HCP and the private key *S* of the patient, respectively. The two-signed copies of the same medical record are then concatenated and together with *m* encrypted by the patient secret key *K,* for confidentiality and consent protection.

$$\mathbf{e}K\{\mathbf{Sign}GS_j(m)//\mathbf{Sign}S(m)//m\}. \quad (1)$$

However, for efficiency enhancement the signature is not performed on the total medical record *m* but on the Hash function of *m*, denoted by *h(m)*. The Hash function of *m* is a control vector, calculated on the basis of *m*, by means of which the integrity (genuineness) of file *m,* can be checked. Changes in the original *m* will lead to a different Hash function *h(m)*. As such, the Hash function is characteristic for the original m and signing *h(m)* has the same

effect as signing *m*, but is less complex since a Hash function is smaller than *m*. The record stored in EPR becomes now,

$$\mathbf{e}K\{\mathbf{Sign}GS_j(h(m))//\mathbf{Sign}S(h(m))//m\}. \quad (2)$$

In the second option, shown in figure 2, a patient signs onto the healthcare provider's (e.g. clinician j) signature. The medical record *m,* itself is also encrypted by the patient's secret key. With a Hash function and employing the HCP group and patient signatures, the medical record stored in the EPR becomes,

$$\mathbf{e}K(m),\ \mathbf{Sign}S(\mathbf{Sign}GS_j\ (h(m))),\ \mathbf{Sign}GS_j(h(m)). \quad (3)$$

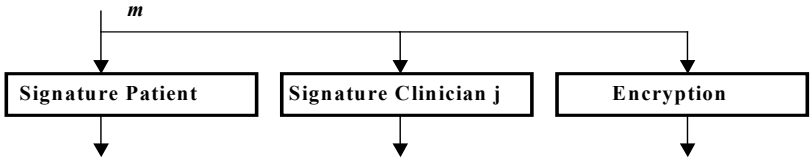


Figure 3. Security mechanism III

For the third option in figure 3 the HCP and the patient each sign the same medical record *m,* and the medical record *m* is encrypted by key *K*. Employing again the Hash function we obtain:

$$\mathbf{e}K(m),\ \mathbf{Sign}GS_j(h(m)),\ \mathbf{Sign}S(h(m)). \quad (4)$$

The three solutions above are similar in that, they do not necessarily need the physical presence of the clinician and patient during the creation of the EPR. They have the same data volume, and verification processes are the same with exception of security mechanism II where one signature verifies another signature. Security III has the minimum risk of total data loss. This makes this solution more attractive than the other two especially when the priority is to rescue the patient life.

6. Conclusion

It has been shown that using crypto mechanisms patient's privacy can be protected. The EPR mechanism that gives better results is the security mechanism III.

Storage type and standardization, data transmission medium security, mobile devices and the possible contents of the patient and HCP hand held mobile assistant devices are some of the issues that need further research and discussions. The same holds for the introduction of different EPR access authorization levels taking into account the differences in sensitivity of the various data types (e.g. less sensitive: demographic data, immunizations etc., sensitive: illness-related information, most sensitive: substance abuse, sexuality, and life style).

References

[1] Gene Itkis. Leonid Reyzin: Forward-Secure Signatures with Optimal Signing and Verifying, In: J. Kilian (ed.), Advances in Cryptology, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, Berlin, Germany, August 2001, p. 332-354

[2] Dawn Xiaodong Song. Practical Forward Secure Group Signature Schemes, In: Eighth ACM Conference on Computer and Communication Security, ACM, November 5-8, 2001, p. 225-234

[3] Gerrit Bleumer, Matthias Schunter. Privacy Oriented Clearing for the German Health Care System, In: Ross Anderson (ed.), Personal Information Security, Engineering and Ethics, Springer-Verlag 1997, p. 175-194

[4]Mihir Bellare, Sara K. Miner. A Forward-Secure Digital Signature Scheme, In: W. Wiener (ed.), Advances in Cryptology, Crypto 99 Proceedings, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, Berlin, Germany, 1999, p. 431-448

[5]Amnon Shabo, Pnina Vortman, Barry Robson. Who's Afraid of Lifetime Electronic Medical Records?, TEHRE 2001 Conference, November 14, London, UK: http://www.haifa.il.ibm.com/~papers.html