Mathematical Problems of Computer Science 37, 83--87, 2012.

Overview of Methods of Biometric Based Key Protection

Gurgen Khachatrian and Narek Malkhasyan

American University of Armenia,
Institute for Informatics and Automation Problems of NAS of RA

Abstract

The security of any modern cryptosystem relies on the assumption that secret keys used for the system such as secret keys for message encryption and authentication as well as private keys of public key cryptosystem are unknown. This assumption is not easy to satisfy in most practical applications. The most widely applicable method uses conventional passwords to encrypt secure keys stored on the computer device. However passwords are vulnerable against many kinds of attacks since they can be either guessed or stolen. Another basic problem is the user authentication. It is well known that when using a traditional and widely used cryptographic methods the user authentication is achieved by challenge - response protocols, the essence of which consists in verifying that the party which wants to confirm his authentication possesses a secret key. In this paper an overview of methods of password generation from biometric data is presented along with the discussion of the remaining challenges and possible directions of future research.

1. Introduction

In most cryptographic algorithms the user authentication is based on possession of some secret, i.e. a user is considered to be legitimate if he owns some kind of decrypting key and can decrypt messages. But cryptographic keys are random and long, thus it is highly impractical (if not impossible) for the user to memorize them. Therefore, the user often stores the key somewhere, for instance, on a hard disk or a flash memory. However, cryptographic keys play a crucial role in the overall security of the system, and once the key gets compromised the entire cryptographic system falls apart. This means that the protection of cryptographic keys, kept on some storage is very important.

The most straightforward way of protecting cryptographic keys is the user authentication via passwords memorized by the user. This is a pretty simple and intuitive way of protecting keys: the user first passes an enrollment process by providing his identity (for instance, the user name) and the password. The system then applies a hash function on the password p, and $hash(p)$ of the password is used to encrypt the user's private key. Afterwards, when the user tries to gain access to his stored encrypted private key, he provides his user name and password to the system and the system applies the same hash function to decrypt the user's private key and as such the user gains access to his private key and he then can be authenticated if the provided password was correct.

While this password-based key release mechanism is very straightforward and intuitive, it also introduces many drawbacks in regard to both security and user convenience. If a password is short, it is easy to guess and it is also vulnerable to dictionary attacks. If a password is long it is hard for the user to remember it, and, at the same time, risky to store. Another drawback is introduced by the fact that many users tend to use the same password in different systems, which means that if the password gets compromised it can be used to gain illegitimate access to those systems. Also traditional passwords hardly can provide a robust level of non-repudiation, as a password is essentially a user knowledge, which can be easily shared with anyone.

Taking into account all the mentioned disadvantages of using traditional passwords for cryptographic key protection, we can consider the most primitive and straightforward usage of biometrics in cryptography: biometric-based key release. The essence of this method is to replace the password authentication module of the previously described mechanism with biometric authentication. Here is how it works: the user first passes an enrollment stage by providing his identity (for instance, the user name) and some biometric information (for instance, the image of his fingerprint). The system then stores the provided biometric information in the database under the user's record. Afterwards, when the user tries to gain access to the stored key, he provides his user name and biometric measurements of the same biological trait. The system applies the biometric matching algorithms to determine if the newly acquired biometric measurements and the measurements stored in the database belong to the same person. If they do, the key is released to the user, otherwise the user is rejected.

As such the main problem for biometric identification and authentication is to generate a password based on some biometric data (fingerprints, DNA, palm vein, iris etc.). There are two basic approaches to this problem. The first approach is based on the generation of passwords based on special robust processing of biometric information. When using this approach the reference data generated during the enrollment stage along with the provided biometric data at the authentication stage produce the same password (i.e. the same binary vector) with very high probability. This approach is discussed in [1, 2]. The second approach [3-5] is based on some kind of processing of biometric data in the way that the reference data generated during the enrollment stage is used to encrypt the secret key. During the authentication stage the data provided is used to decrypt the secret key and the decryption is successful if the significant portion of provided biometric data coincides with the biometrics at enrollment stage. In the next section we will discuss both approaches in more detail.

2. Short Review of Generation of Passwords from Biometric Data

We will start our analysis with the second approach. The most important result in this direction is the concept of "fuzzy vault" presented by A. Juels and M. Sudan [4]. The main idea behind this scheme is the following. Suppose there is a secret that is represented as a polynomial of degree less than k over finite field $GF(q)$. For example, if the secret is a 256-bit vector and $q = 2^{16}$ we have to consider the secret as a polynomial over $GF(2^{16})$ with degree not more than 15, i.e. $P(x) = a_0 + a_1x + \cdots + a_{15}x^{15}$ where $a_i \in GF(2^{16})$. Then the secret polynomial is encoded by generalized Reed-Solomon codes as follows: the secret polynomial is evaluated over any set of distinct points over $GF(q)$ and a codeword represents a set of pairs $\{x_i, y_i\}$ where $x_i \in GF(q)$ and $y_i = P(x_i)$. It is well known that Hamming distance d for corresponding Reed-Solomon codes is equal to $t - k + 1$ and therefore up to $(d-1)/2 = (t-k)/2$ errors can be corrected. This means that if in the process of decoding there will be at least $(k+t)/2$ correct pairs $\{x_i, y_i\}$, the polynomial $P(x)$ will be successfully decoded. This concept is the heart of the so called "fuzzy vault" scheme meaning that the vault will be opened or the secret ll be recovered if the significant portion of corresponding evaluation points of the polynomial correct, where that portion is determined by the parameters of underlying Reed-Solomon code, t and k. The next step is to conceal the codeword representing a secret polynomial by adding so called chaff points, i.e. random noise in the form of $\{x_i, y_i\}$ pairs and a parameter r, hich is in fact the number of the added chaff points, where $r < q$. As such the fuzzy vault heme is characterized by the parameter triple (k, t, r). This scheme can be used for generating sswords from biometrics in the following way. As an example suppose we wish to generate sswords from fingerprints. It is well known that fingerprints can be represented by minutiae ints, and coordinates of minutiae points can be represented as elements of the field $GF(q)$. In most typical setting both horizontal and vertical coordinates of minutiae points can be resented in one byte: so the overall minutiae coordinate can be represented as an element of (2^{16}). Also in most cases it is enough to encode a fingerprint with 21 minutiae points. Now ppose that during the enrollment process a user provides his fingerprint and as a result 21 nutiae points are generated. These minutiae points x_i are used to encode, then to calculate the aluation of the secret polynomial for those points to get pairs $\{x_i, y_i\}$. If the secret lynomial is of degree 15 but we have 21 pairs, then the parameters of the corresponding Reed-llomon code are $t = 21$ and $k = 15$, and therefore the correcting capability of that code would 3 errors. Also in addition chaff points are added to that set to insure the security of the system. w if the user wants to be authenticated, i.e. wants to release the secret key, he provides his gerprint and the corresponding 21 minutiae points are generated. If 18 out of 21 minutiae ordinates are correct, then the secret is released.

should be noted that the above construction works for unordered sets, which means that the ative positions of set elements do not change the characteristic of the set, which in its turn ans that, for example, in the case with minutiae their respective position does not play any e. This is a significant improvement compared to the work by Juels and Wattenberg [3], where order of elements is important.

other approach to the problem of generation of passwords from biometric data, which also s fuzzy vault ideas, is demonstrated in the work [5]. Unlike the work [4], this work is not ing any error correction technique described in the previous paragraph. The implementation of zy vault is again carried out using fingerprint minutiae features. In this scheme the secret data is encoded by "Cyclic Redundancy Check" (CRC) polynomial. This is a commonly used hnique in communication channels, in particular in TCP/IP protocol to detect a burst of errors to a certain length. 16-bit CRC data is appended to the secret S (128 bits) to construct 144-SC. In this way all burst of errors up to the length 16 will be detected.

$X) = x_{16} + x_{15} + x_2 + 1$ is used to generate 16-bit CRC symbols. 144 bit SC is resented as a polynomial of degree 9 over $GF(2^{16})$ i.e. $P(u) = c_0 + c_1 u + \cdots + c_8 u^8$. The nuine set G is then found by evaluating $P(u)$ on the template minutiae features. As such we d that $G = \{(u_1, p(u_1)), \ldots, (u_N, p(u_N))\}$. Chuff points as in the previous case are added for security of the system. These are randomly selected points that do not overlap with genuine ints along with other points that do not fall with evaluation of $P(u)$ for these points. Thus the ult is the union of these two sets, shuffled in random order. The decoding procedure is as llows: for the query minutiae $u_1^* \ldots u_N^*$ the points to be used for polynomial reconstruction are und by comparing u_i^*, $i = 1 \ldots N$ with the abscissa of the vault V. If any u_i^* is equal to some st coordinate of V, the corresponding vault point is added to the list of points to be used. sume that the list has K points, where $K \leq N$. It is well known that for decoding D degree lynomial $D + 1$ unique evaluations are necessary. For each of (K choose $D + 1$) combinations Lagrange interpolating polynomial should be constructed. After construction of the rresponding polynomial we should check whether there are errors in the secret by dividing the obtained polynomial by $P(X) = x_{16} + x_{15} + x_2 + 1$. If the reminder is zero, there are n errors with very high probability. If the query minutiae list overlaps with template minutiae li in at least $(D + 1)$ points, for some combinations, the correct secret will be decoded and reveale to the legitimate user.

The drawback of this approach is that many combinations (K choose $D + 1$) of Lagrang interpolating polynomial should be constructed until the correct one is obtained. Anoth drawback is the complexity of locating possible errors by using Reed–Solomon codes.

Now let us analyze the first approach as it was explained at the end of the previous section. this case the idea is to generate encryption keys by using reference biometric information, whic will be used as a password to encrypt secret information with either symmetric 128 or 256 b key or a private key for the public key system. In the paper [2] a method of generating keys fro fingerprint images is demonstrated. Instead of minutiae based processing of fingerprints a nov approach for template selection methodology is proposed, based on specific features of t templates with high uniqueness. Analyses show that for the unique templates there is a specif distribution of similar patterns. The most similar templates, which are deterministic for countin the final uniqueness of the template, are located close to the original. After the enrollment sta the most unique templates are calculated and stored in database. The testing results show that such templates are sufficient in most cases. Passwords are generated based on these templates combination with genuine fingerprint images. It is shown that the 84 bit password can reliably generated. The security of the system is analyzed from two points of view. At first, was found that the proposed system had fairly low "false acceptance rate" (which could be ma as low as 0.01%). This is due to two-step verification. First, the system aligns templates on t secondary image and counts the accuracy of the fitting. If this value is less than the predefin threshold value, this person is not authenticated. At the second phase the algorithm generates password based on the template locations. These passwords should be exact; otherwise, the us is again rejected.

3. Conclusion and Directions for Future Research

In this paper a brief review of different approaches to the problem of generating passwords fr biometric information is presented. An interesting research direction would be the investigati of methods of using the ideas presented in the paper [2] in case of other types of biometrics, example, the palm vein biometrics. Another interesting direction would be a detailed comparis of two approaches reviewed in this paper in terms of complexity of implementation and securit

4. Acknowledgment

This research has been carried out within the project "*Application of Security to Biometrics a Communications*", sponsored by the Volkswagen Foundation.

References

1. M. Maslennikov, *Practical Cryptography*, Saint Petersburg, 2003.
2. G. Khachatrian and H. Khasikyan "Correlation based password generation from Fingerprin *Proc. ITA-2012 conference "Classification, Forecasting, Data Mining "*.
3. A. Juels and M. Wattenberg, "A fuzzy commitment scheme", *In Sixth ACM confere Computer and Communication Security*", pp. 28-36, 1999.

4. A. Juels and M. Sudan, "A fuzzy vault scheme" , *Proc. IEEE International Symposium on Information Theory"* , pp.408, 2002.
5. U. Uludag, S. Pankanti and A. Jein. "Fuzzy vault for fingerprints", *Lecture Notes on Computer Science*, pp. 55-71, 2005.

Բանալիների պաշտպանության բիոմետրիկ (կենսաչափական) մեթոդների դիտարկում

Գ. Խաչատրյան և Ն. Մալխասյան

Ամփոփում

անկացած ժամանակակից կրիպտոհամակարգի անվտանգությունը հիմնվում է այն թադրության վրա, որ համակարգում օգտագործվող բանալիները, ինչպես օրինակ՝ աղորդագրությունների գաղտնագրման, նույնականացման և բաց բանալիով իպտոհամակարգերի բանալիները, անհայտ են: Կիրառական համակարգերի ծամասնությունում այս ենթադրությունը բավարարելը հեշտ չէ: Ամենատարածված թոդը ավանդական գաղտնաբառերի օգտագործումն է համակարգչային սարքի վրա ահվող բանալին գաղտնագրելու համար: Սակայն գաղտնաբառերը խոցելի են արատեսակ հարձակումների նկատմամբ, քանի որ դրանք կարող են գուշակվել և ողացվել: Մեկ այլ կարևոր խնդիր է օգտագործողների նույնականացման խնդիրը: Հայտնի որ ավանդական և տարածված ծածկագրաբանական մեթոդներ օգտագործելիս տագործողի նույնականացումը իրականացվում է <<մարտահրավեր-պատասխան>> րձանագրությունների միջոցով, որոնց օգնությամբ օգտագործողը կարող է ապացուցել ևէ բանալու պատկանելությունը իրեն: Սույն հոդվածում ներկայացված են բիոմետրիկ (կենսաչափական) տվյալներից գաղտնաբառերի ստացման մեթոդների, ինչպես նաև որոշ այլ մարտահրավերների և աշխատանքի ապագա հնարավոր ուղղությունների տարկումները:

Обзор биометрических методов защиты ключей

Г. Хачатрян и Н. Малхасян

Аннотация

езопасность всех современных криптосистем базируется на предположении, что кретные ключи используемые в системе, такие как ключи для шифрования юбщений, ключи аутентикации и ключи криптосистем с открытым ключом, известны. В большинстве практических приложений удовлетворять это редположение непросто. Самый распространенный метод - это использование радиционных паролей для шифрования ключей хранящихся на некоторых омпютерных устройствах. Но пароли уязвимы множеством атак, так как они могут ыть разгаданы и украдены. Другая основная проблема заключается в аутентикации ользователей. Хорошо известно, что при использовании традиционных и широко звестных криптографических методов, аутентикация пользователей достигается при омощи протоколов "вызов-ответ", при помощи которых пользователь может доказать ринадлежность некоторого ключа ему. В этой статье представляется обзор методов енерирования паролей из биометрических данных, а также рассматриваются вызовы в гой сфере и возможные будущие пути исследования.