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.

References

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

Ցանկացած ժամանակակից կրիպտոհամակարգի անվտանգությունը հիմնվում է այն ենթադրության վրա, որ համակարգում օրտագործվող բանալիները, ինչպես օրինակ՝ հաղորդագրությունների գաղտնագրման, նույնականացման և բաց բանալիով կրիպտոհամակարգերի բանալիները, անհայտ են: Կիրառական համակարգերի մեծամասնությունում այս ենթադրությունը բավարարելը հեշտ չէ: Ամենատարածված մեթոդը ավանդական գաղտնաբառերի օգտագործումն է համակարգչային սարքի վրա պահվող բանալին գաղտնագրելու համար: Սակայն գաղտնաբառերը խոցելի են տարատեսակ հարձակումների նկատմամբ, քանի որ դրանք կարող են գուշակվել և գողացվել: Մեկ այլ կարևոր խնդիր է օգտագործողների նույնականացման խնդիրը: Հայտնի է, որ ավանդական և տարածված ծածկագրաբանական մեթոդներ օգտագործելիս օգտագործողի նույնականացումը իրականացվում է <<մարտահրավեր-պատասխան>> արձանագրությունների միջոցով, որոնց օգնությամբ օգտագործողը կարող է ապացուցել որևէ բանալու պատկանելությունը իրեն: Սույն հոդվածում ներկայացված են բիոմետրիկ (կենսաչափական) տվյալներից գաղտնաբառերի ստացման մեթոդների, ինչպես նաև ոլորտի այլ մարտահրավերների և աշխատանքի ապագա հնարավոր ուղղությունների դիտարկումները:

Обзор биометрических методов защиты ключей

Г. Хачатрян и Н. Малхасян

Аннотация

Безопасность всех современных криптосистем базируется на предположении, что секретные ключи используемые в системе, такие как ключи для шифрования сообщений, ключи аутентикации и ключи криптосистем с открытым ключом, неизвестны. В большинстве практических приложений удовлетворять это предположение непросто. Самый распространенный метод - это использование традиционных паролей для шифрования ключей хранящихся на некоторых компютерных устройствах. Но пароли уязвимы множеством атак, так как они могут быть разгаданы и украдены. Другая основная проблема заключается в аутентикации пользователей. Хорошо известно, что при использовании традиционных и широко известных криптографических методов, аутентикация пользователей достигается при помощи протоколов “вызов-ответ”, при помощи которых пользователь может доказать принадлежность некоторого ключа ему. В этой статье представляется обзор методов генерирования паролей из биометрических данных, а также рассматриваются вызовы в этой сфере и возможные будущие пути исследования.