DEMO: Gradiant Asymmetric Encryption and Verification Systems based on Handwritten Signature

Enrique Argones Rúa, Francisco Javier García Salomón, Luis Pérez-Freire
GRADIANT - Galician Research and Development Center in Advanced Telecommunications
Edificio CITEXVI, local 14, Campus Universitario de Vigo
36310 Vigo, Pontevedra, Spain
{eargones,fgarcia,lpfreire}@gradiant.org

ABSTRACT

A successful deployment of biometric-based recognition systems in real-life applications depends on crucial issues such as data security and privacy, which have to be specifically addressed. Besides, cryptographic key protection can represent the main weakness of a secured transmission. In this demonstration a system for encryption and digital signature of generic digital documents (SAES, standing for Signature-based Assymetric Encryption System) is presented, where cryptographic keys are protected by the hand-written signature of the user. Furthermore, a demonstration of a the handwritten online signature verification system (SVS) based on non-protected templates will also be performed.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication*; K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*

Keywords

Cryptobiometrics, handwritten signature verification, Hidden Markov Models

1. TECHNOLOGY TO BE DEMONSTRATED AND ITS NOVELTY

Two systems will be demonstrated. The first one is a online signature verification system based on generative models. The second one is a cryptosystem online signature verifier, which uses protected and renewable templates. A similar demonstration was performed in the IEEE Workshop on Information Forensics and Security held in Tenerife in December 2013, where only the Signature-based Assymetric Encryption System (SAES) was presented. In this demonstration the Signature Verification System (SVS) is also shown, and it includes several new features that increase robustness against forgeries.

CCS'13, November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11.
http://dx.doi.org/10.1145/2508859.2512497.

The SVS, based on unprotected HMM templates, uses a user-specific HMM for state-sequence score computation, and a adapted HMM-Universal Background Model (UBM) for loglikelihood ratio score computation, as described in [1]. This combination obtains very low error rates, as demonstrated by the UVIGO system performance in the Biosecure Signature Evaluation Campaign (ESRA'2011) [3], and high resistance against high quality forgeries. This verification system is designed to work with a variable number of enrollment signatures (from a single signature enrollment to 5 enrollment signatures). Enrollment is performed using a stability maximization approach, in order to avoid outlier signatures to become part of the user template. This provides user templates with increased ressistance to forgeries. Besides, user template quality is evaluated, what provides useful information regarding its security or ressistance to attacks. Templates are classified after the enrollment into three different security levels, namely low, medium and high security level.

The protected system (SAES) is mainly based on the template protection scheme presented in [2]. The system uses a set of UBM as system parameters. User templates are obtained from the biometrics captured in the enrollment phase, and they depend on the set of UBMs and their corresponding eigen-model matrices. Only a protected and non-invertible version of the biometric user template and cryptographic private key is stored in the system's database, so there is not need for special protection of the system's database.

The signature of the user is used in the test phase to recover the hashed private key, so document decryption and digital signature rely on the presentation of the user's signature to the system. The block diagram of the system is shown in Figure 1, where both enrollment and test phases are illustrated.

The current version of the system produces biometric keys with an effective length of 99 bits (the k parameter in the $BCH(n,k,t)$ code) using only 5 enrollment signatures, which is more than enough to protect a 1024-bit length RSA or DSA key. Biometric verification performance is also kept in acceptable rates, with an $EER\% = 4.61$, as shown in Figure 2. These figures are better than those obtained by the system presented in [2] (biometric keys with an effective length of 76 bits when using 10 enrollment signatures, $EER\% = 4.41$). This is mainly because of the substitution of the reliable coefficients selection approach used in [2] by a new combination approach, where the most reliable projections are combined using a greedy algorithm to obtain n equally reliable features.

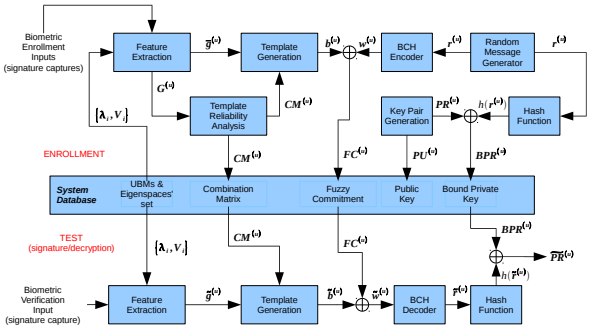

Figure 1: Block Diagram of the Gradiant Asymmetric Encryption System, showing the private key binding and retrieval mechanisms

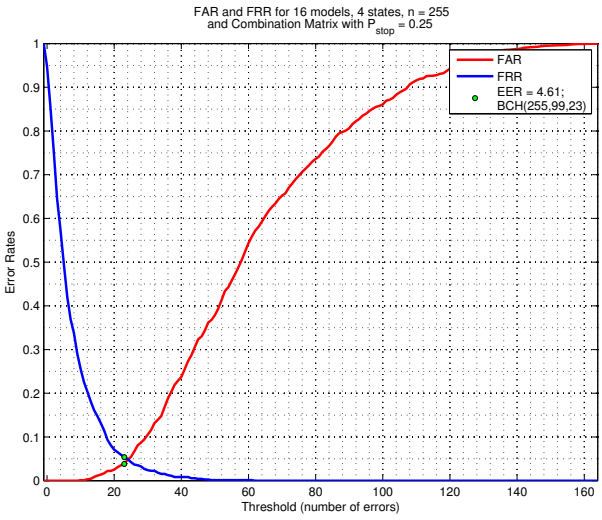

Figure 2: System performance when using a BCH code with $n = 255$. Many feasible working points are available. The working point closest to the EER is labeled with a green circle.

Figure 3: Picture of a user during the enrollment phase of the Gradiant Asymmetric Encryption System based on handwritten signature.

The system has been deployed on a desktop application using Qt [4], so it is available for Windows (XP, Vista, 7), Linux and MacOS. A Wacom Intuos 4 S [5] is used for signature capture for the protected templates system, and a Wacom STU-500 is used for signature capture for the unprotected system. The demonstration applications will be installed in a Laptop. Figure 3 shows a person using the system for capturing his handwritten signature of the protected system. Both the capture device and the laptop running the application will be provided by the demonstrator.

2. INTERACTIVITY WITH THE AUDIENCE

The demonstrator will first show the main features of the application, but the user's participation is very important in the demonstration: volunteers for enrolling, testing (document signing or decryption), or to imitate other user's signatures in order to overcome the cryptographic key protection will be welcome.

3. ACKNOWLEDGMENTS

This work was partially supported by the LIFTGATE Project funded by the FP7-Capacities Programme, Grant Agreement No. 285901.

4. REFERENCES

[1] E. Argones Rua and J. Alba Castro. Online signature verification based on generative models. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 42(4):1231–1242, 2012.

[2] E. Argones Rúa, E. Maiorana, J.L. Alba Castro, and P. Campisi. Biometric template protection using universal background models: An application to online signature. 7(1):269–282, 2012.

[3] N. Houmani, S. Garcia-Salicetti, B. Dorizzi, J. Montalvao, J. C. Canuto, M. V. Andrade, Y. Qiao, X. Wang, T. Scheidat, A. Makrushin, D. Muramatsu, J. Putz-Leszczynska, M. Kudelski, M. Faundez-Zanuy, J. M. Pascual-Gaspar, V. Cardenoso-Payo, C. Vivaracho-Pascual, E. A. Rua, J. L. Alba-Castro, A. Kholmatov, and B. Yanikoglu. Biosecure signature evaluation campaign (esra'2011): evaluating systems on quality-based categories of skilled forgeries. *Biometrics, International Joint Conference on*, 0:1–10, 2011.

[4] Nokia Corporation. Qt, 2008.

[5] Wacom Company, Ltd. of Tokyo, Japan. Wacom Intuos 4 S, 2012.