Morning Tutorial 1: Privacy Preserving Biometric Identity Verification

Abstract

Biometric identify verification systems provide many advantages over conventional password-based authentication systems. Unlike the latter, which could be forgotten or pilfered, the former are based on indelible physical attributes, and are not dependent on potentially faulty memory.

On the other hand, biometric authentication systems come with privacy risks. The authenticating server now possesses an equally indelible biometric signature of the subject. The server, or any malicious adversary who manages to “steal” the signature from it, or even a legal entity who subpoenas the server, could abuse these signatures in a variety of ways, such as using them to identify the subject in other unauthorized contexts (e.g. searching for their faces of voices on YouTube videos, or matching fingerprints in potential crime scenes), creating fake signals (e.g. synthetic voices or fingerprints) that could then be used to authenticate as the user, etc.

The need, then, is for secure biometric authentication systems in which guarantees exist that the biometric signatures of users possessed by the system cannot be abused even by the system itself.

The obvious solution is to encrypt the biometric signatures at the server, such that the server itself (let alone any third-party entity who accesses the server) cannot decrypt it, and to perform the biometric matching at the server using encrypted signatures themselves. This is a task for “homomorphic encryption” – encryption techniques that enable computations such as matching in the encrypted domain. Homomorphic encryption techniques, however, remain practically infeasible, in spite of recent progress in the area.

The purpose of this tutorial is to review the current issues and describe alternative and complementary approaches to homomorphic encryption for secure biometric authentication. In this context we will briefly review several techniques including secure multiparty computation, oblivious transfer, zero-knowledge proofs, garbled circuits, locality sensitive hashing, and binary embeddings, and also discuss computational and performance tradeoffs. Cancellable and revocable biometrics will also be reviewed.

Presenters

Dr. Gérard Chollet studied Linguistics, Electrical Engineering and Computer Science at the University of California, Santa Barbara where he was granted a PhD in Computer Science and Linguistics. He taught at Memphis State University and University of Florida before joining CNRS. In 1981, he was asked to take in charge the speech research group of Alcatel. In 1983, he joined a newly created CNRS research unit at ENST. The group contributed to a number of European projects such as SAM, ARS, FreeTel as well as national projects. In 1992, he was asked to take in charge the speech research group of Alcatel. In 1983, he joined a newly created CNRS research unit at ENST. The group contributed to a number of European projects such as SAM, ARS, FreeTel as well as national projects. In 1992, he was asked to participate to the development of IDIAP, a new research laboratory of the 'Fondation Dalle Molle' in Martigny, Switzerland. IDIAP contributed to SpeechDat, M2VTS and other European projects. From 1996 to 2012, he was full time at ENST, managing research projects and supervising doctoral work. Funding was secured from such projects as Eureka-Majordome and MajorCall, NoE-BioSecure, Strep-SecurePhone, IP-Companion@ble, AAL-vAssist, FET-ILHAIRE,... He supervised more than forty doctoral thesis. CNRS decided in july 2012 to grant him an emeritus status. He visited Boise State University in 2013 and the University of Eastern Finland in 2014. He is now VP of Res. of Intelligent Voice (http://www.intelligentvoice.com/).
Dijana Petrovska-Delacrétaz obtained her degree in Physics and her PhD from the Swiss Federal Institute of Technology (EPFL) in Lausanne. She was working as a Consultant at AT&T, as a post-Doc at Télécom ParisTech, and as a Senior Scientist in the Informatics Department of Fribourg University, Switzerland. Since 2004 she is an associate professor in Mines Télécom / Télécom SudParis. Her research activities are oriented towards pattern recognition, signal processing, and data-driven machine learning methods, that are exploited for applications such as speech, speaker and language recognition, very low-bit speech compression, biometrics (2D and 3D face, and voice), and privacy preserving biometrics (cancelable biometric and generation of cryptographic keys from biometric data). Her publication list is composed of three patents, two publicly available databases (for speaker recognition and biometrics evaluations), open-source software for reproducible results, 81 publications, and co-supervision of five PhD thesis.

Bhiksha Raj is an Associate Professor in the Language Technologies Institute of the School of Computer Science at Carnegie Mellon University, with additional affiliations to the Electrical and Computer Engineering and Machine Learning departments. Dr. Raj obtained his PhD from CMU in 2000 and was at Mitsubishi Electric Research Laboratories from 2001-2008. Dr. Raj’s chief research interests lie in automatic speech recognition, computer audition, machine learning and data privacy. Dr. Raj’s latest research interests lie in the newly emerging field of privacy-preserving speech processing, in which his research group has made several contributions.

Topics
i. Introduction to Privacy Preserving Biometric Authentication
ii. Cancellable / Revocable biometrics
iii. A brief review of cryptology
iv. Matching in the encrypted domain,
v. Homomorphic encryption, Secure Multi-party Computation
vi. Masking, Oblivious Transfer, Zero Knowledge Proofs
vii. Garbled circuits
viii. Locality Sensitive Hashing, Secure Binary Embeddings
ix. Applications, Multi-modal biometrics
x. Evaluations, Spoofing and other attacks
xi. Conclusions and Perspectives

References
- S. Ganeh Kanade, D. Petrovska-Delacrétaz, B. Dorizzi. Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data; in IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR); June 2009

