Advanced Cryptographic Key Generation from Passwords and Biometric Data

Sébastien Canard (Télécom Paris)

Context

In modern cryptography, the secure generation and management of cryptographic keys are critical to ensuring data confidentiality, integrity, and authentication. Traditional key generation methods often rely on random number generators or pre-shared secrets, but these approaches can be vulnerable to attacks or impractical for human users, especially when the cryptographic key is then used to secure data through a web browser. Two promising alternatives are password-based key derivation functions (PBKDFs) and biometric-based key generation using fuzzy extractors. PBKDFs, such as PBKDF2, Argon2, and scrypt, derive cryptographic keys from human-memorable passwords, balancing security and usability. However, they remain vulnerable to brute-force and dictionary attacks if the password is weak. It also poses some big issues when the user has forgotten their password. On the other hand, biometric data (e.g., fingerprints, iris scans) offers a unique and user-friendly approach to key generation. Yet, biometric data is inherently noisy and variable, requiring specialized techniques like fuzzy extractors to reliably reproduce keys from imperfect inputs. But those techniques are not yet enough mature to be largly deployed. This project explores the state-of-the-art in both domains, aiming to analyze, improve, and implement secure and practical key generation techniques.

Objectives

- Literature Review: Study existing PBKDFs (e.g., PBKDF2, Argon2, scrypt) and their security properties. Explore fuzzy extractor schemes for biometric key generation, focusing on error tolerance and security guarantees.
- Analysis and Comparison: Compare the strengths and weaknesses of password-based and biometric-based key generation. Identify potential vulnerabilities or limitations in current approaches.
- Improvement or Innovation: Propose enhancements to existing PBKDFs or fuzzy extractors, to manage loss of password, to improve fuzzy extractor technique, or to see whether a hybrid approach combining passwords and biometrics could be relevant.
- Implementation: Implement one or more selected PBKDFs and fuzzy extractor schemes in a chosen programming language (e.g., Python, C++), and test the implementations for correctness and performances.

Practical Information

Regular meetings will be scheduled with the advisors, either via visioconference or in Palaiseau. If you are interested, send an email to `sebastien.canard@telecom-paris.fr`.