Authentication Attacks on Projection Based Cancelable Biometric Schemes

DURBET Axel, GROLLEMUND Paul-Marie, LAFOURCADE Pascal, MIGDAL Denis and THIRY-ATIGHEHCHI

Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS, LMBP France

SCAN ME

Objectives

1. Contruct an impersonation attack on CB scheme.
2. Formalize how to consider the filter in such attack.
3. Show attacks on some projection-based cancelable biometric schemes.

Introduction

- Biometric authentication is widely used.
- It is more convenient and quicker.
- Biometric characteristics cannot be lost.
- Biometric characteristics cannot be forgotten.
- This solution are not exempt from vulnerabilities.
- The projection-based cancelable biometric schemes are very common.
- Some theoretical attacks are provided.

Materials

- Python 3.9.
- Gurobi 9.1.2.
- Debian 11.
- EPYC 7F72 dual processor (48 cores).
- 256GB RAM.

Attacked Scheme

- The attacked CB instantiation, described in our Algorithm, is based on a uniform random projection (*URP*). Such a projection serves as an embedding of a high-dimensional space into a space of much lower dimension while preserving approximately the distances between all pairs of points.
- Here is the attacked algorithm based on Sobel filter:

Algorithm 1 [URP-SOBEL]

Inputs : biometric data I; token parameter P
Output : BCV vector $T = (t_1, \dots, t_m)$

Apply Sobel filter on I to produce an n-sized feature vector: $F = (f_1, \dots, f_n)$.
Generate with the token P a family V of m pseudorandom vectors $V_1, \dots, V_m$ of size n according to a uniform law $\mathcal{U}([-0.5, 0.5])$.
Arrange the family V as a matrix M of size $n \times m$.
Compute T as the matrix-vector product $F \times M$.
for t_i in T **do**
    if $t_i < 0$ **then** $t_i = 0$ **else** $t_i = 1$
end for
return T

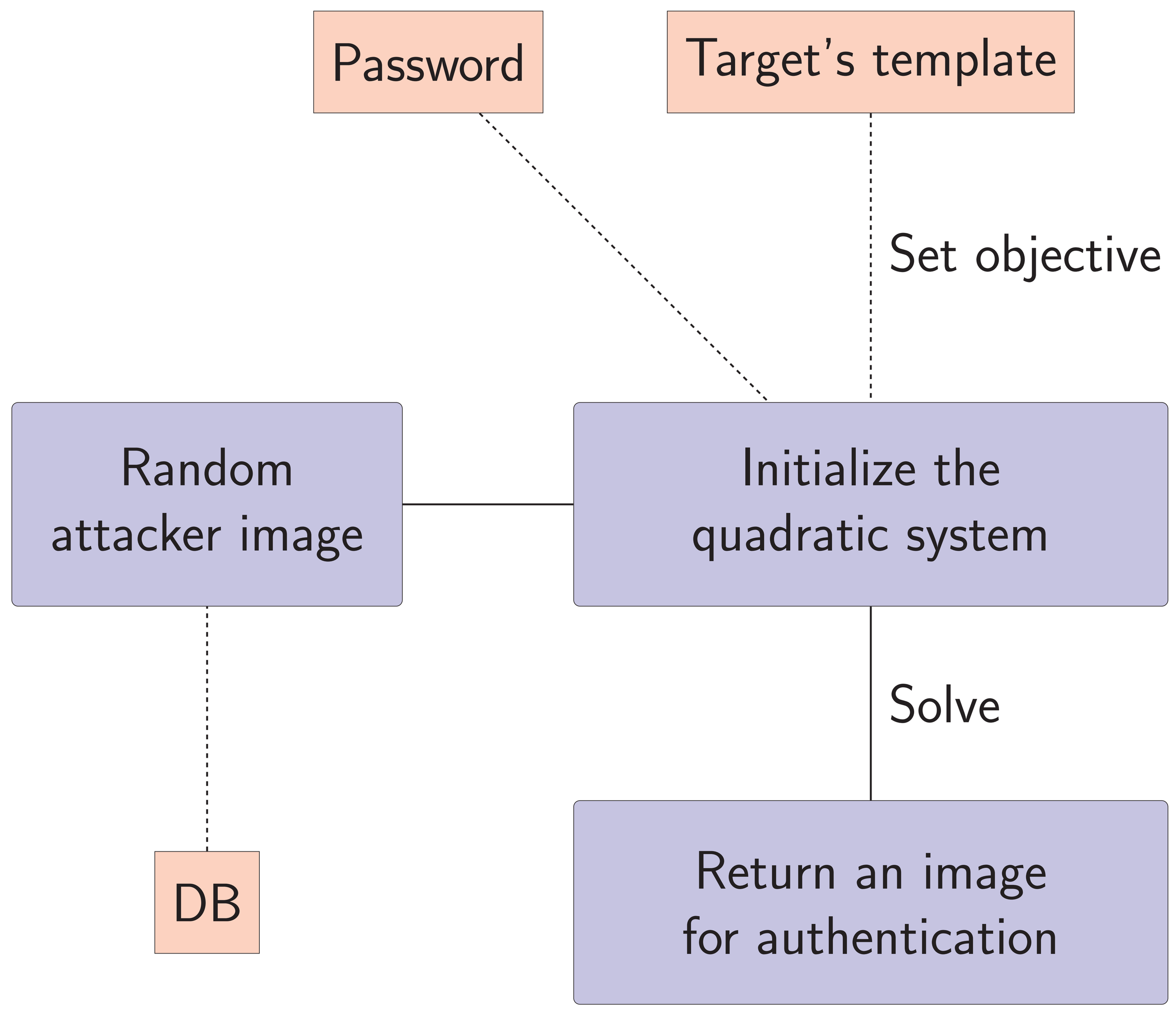
Mathematical Section

- Assume that $I_A = (o_{i,j})_{n\times m}$ is the attacker's original image, $I' = (x'_{i,j})_{n\times m}$ the modified original image and $X = (x_{i,j})_{n\times m}$ its augmented form. Let $\mathcal{K}_1$ be all indices where the template is equal to 0 and $\mathcal{K}_2$ all other indices. Let $M = (a_{i,j})_{(n*m)\times \ell}$ be the projection matrix. Let Y_{flat} be the flattened form of the matrix Y where rows are concatenated in a single vector.
- The attack consists of solving following problem for Sobel filter:
  - Minimize: $\|X - I_A\|^2$
  - Subject to the following constraints:

$$\begin{cases} Y^2 = \left[(G_1 * X)^2 + (G_2 * X)^2\right] \\ Y_{flat} M_i < 0, \forall i \in \mathcal{K}_1 \\ Y_{flat} M_j \geq 0, \forall j \in \mathcal{K}_2 \\ x_{i,j} \in \{0, \dots, 255\}, \forall (i,j) \end{cases}$$

Sobel Filter Example

Attack Overview



Beginning of Result

Image Size	Mean Distance	Mean Time (s)
2×2	99	0.14
2×3	117	32.76
3×3	133	150.0
4×3	144	146.67
4×4	177	150.0

Table 1:Summary of the experiments for a 50-bit template.

Conclusion

- Several authentication attacks on a popular CB scheme has been presented.
- Attacks are conducted on a complete chain of treatments.
- Two ways for the attacker to impersonate several legitimate persons has been presented.
- The modification of the attacker's image is minimal.

Future Work and How to Ensure the Scaling of the Attack

- Code optimization.
- System relaxation.

Acknowledgments

The authors acknowledges the support of the French Agence Nationale de la Recherche (ANR), under grant ANR-20-CE39-0005 (project PRIVABIO).

Contact Information

- Web: PRIVABIO Project on: https://privabio.limos.fr/
- Email: axel.durbet@uca.fr