Bezpieczne przechowywanie wzorca biometrycznego

na karcie elektronicznej

Bibliografia

Capacity and Examples of Template-Protecting Biometric Authentication Systems

Pim Tuyls and Jasper Goseling, 2004

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.4.7263

Identyfikacja biometryczna

- odcisk palca
- tęczówka oka
- głos
- sposób chodzenia

- danych nie można zapomnieć lub zgubić!

Zagrożenia wynikające z przechowywania danych biometrycznych

- Podszycie się
  - po kradzieży danych biometrycznych, napastnik może wyprodukować sztuczne urządzenia biometryczne
- Niemożliwe odzyskanie
  - raz utracone dane biometryczne stają się bezużyteczne, nie można ich zmienić, wydać na nowo, czy zniszczyć
- Wydanie
  - wrażliwych danych osobistych

Wymagania bezpieczeństwa

1. Dane przechowywane w bazie danych nie mogą być wystarczające do podszycia się
2. Dane przechowywane w bazie danych zawierają możliwie najmniej informacji biometrycznych i poufnych

Architektura spełniająca te wymagania zapewnia pełne bezpieczeństwo właściwych danych biometrycznych.

Dane pomocnicze i referencyjne

- Ze względu na występujące zakłócenia, proces pozyskiwania danych biometrycznych wymaga wielokrotnego skanowania cechy. Podczas pozyskiwania danych tworzy się **dane pomocnicze** zawierające możliwie ogólny wzorzec cechy (unikalny łańcuch znaków) - pozwalający na wygodne wykorzystywanie biometrii do uwierzytelniania
- Fragmenty danych będące najbardziej istotne (pozwalają na jednoznaczną identyfikację tożsamości) są haszowane i zapisywane jako zupełnie niezależne od danych pomocniczych **dane referencyjne**

Secret Extraction Codes (SECs)

Zdefiniujmy **n,ε > 0** i **Xn i Yn** jako alfabety wejściowy i wyjściowy, **S** jako zbiór sekretów.

SEC **c (n,lSl,ε)** zdefiniowany na **Xn x Yn** to uporządkowany zbiór par kodowania i odkodowywania

C ={(Ei,Di)li = 1,2,…,lSl}

gdzie **Ei ⊆Xn** i **Di ⊆Yn** i spełniają:

$$\mathcal{E}_i \cap \mathcal{E}_j = \emptyset, \qquad \mathcal{D}_i \cap \mathcal{D}_j = \emptyset, \qquad \bigcup_i \mathcal{D}_i = \mathcal{Y}^n,$$

dla **i,j = 1,2,...,lSl, i/= j** i **$P_{Yn|Xn}(D_i|x^n_i) \geq 1 - \varepsilon$,**

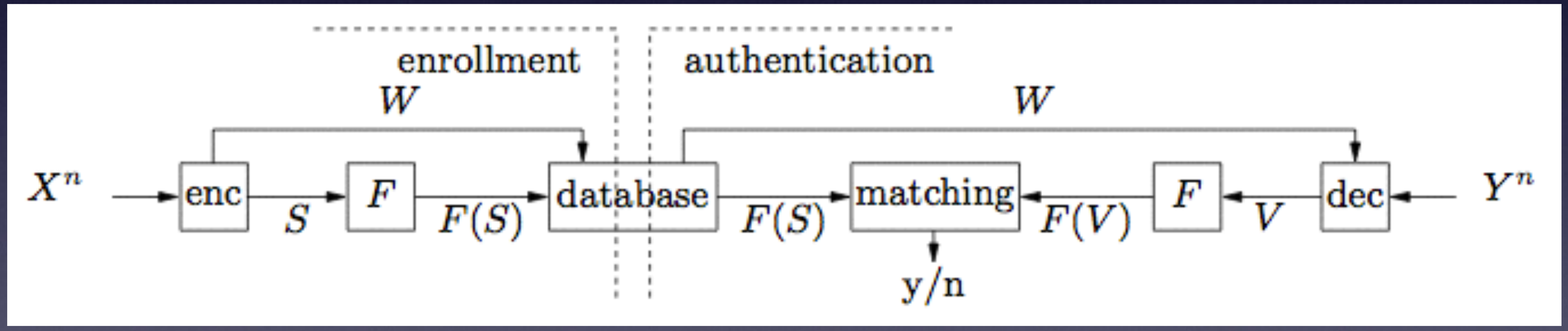
dla każdego **$x^n_i \in E_i$, oraz i = 1,2,…,lSl**

Secret Extraction Codes (SECs)

SEC zapewnia schemat kodowania-dekodowania zmiennej (także ciągłej) na skończony alfabet **S = {1, 2, . . . , |S|}** poprzez dyskretyzację. Przy przedstawionych założeniach zapewnia jednoznaczne kodowanie i dekodowanie.

SECs są zbliżone do kodów geometrycznych, .

Algorytm SBA
(Secure Biometric Authentication Algorithm)



Algorytm SBA
(Secure Biometric Authentication Algorithm)

Pozyskiwanie danych

Zdefinujmy $\mathbf{\Phi}_n \subseteq \mathbf{C}$, $\mathbf{SEC\ C = \{(E_i,D_i)\}^{|S|} \in \Phi_{xn}}$ jeżeli $\mathbf{x^n \in E_i}$

1. Dane biometryczne ($\mathbf{x^n}$) użytkownika są pobierane, dane pomocnicze (**w**) wyodrębniane.
2. Wybierany jest losowy Secret Extraction Code (SEC) ze zbioru $\mathbf{\Phi_{xn}}$, jego indexem ustawiany jest ciąg znaków - dane pomocnicze (w), jeżeli $\mathbf{\Phi_{xn} = \varnothing}$, wybierany jest losowy SEC z **C**
3. (x^n) zostają zakodowane kodem SEC, tak by uzyskać sekret (s): Mając $\mathbf{C = \{(E_i,D_i)\}^{|S|}}$ sekret **s** definiowany jest jako **s = i** jeżeli $\mathbf{x^n \in E_i}$, gdy $\mathbf{\Phi_{xn} = \varnothing}$, jest losowany.
4. Jednokierunkowa funkcja haszująca F jest stosowana do sekretu s. Zahaszowane dane referencyjne, dane pomocnicze i metadane użytkownika są zapisywane do bazy danych.

Algorytm SBA
(Secure Biometric Authentication Algorithm)

Uwierzytelnianie

1. Użytkownik podaje swoją tożsamość.
2. Zaszyfrowane funkcją F dane referencyjne(F (s)) i dane pomocnicze (w) są pobierane dla potencjalnego użytkownika.
3. Dane biometryczne użytkownika (y^n) wraz z danymi pomocniczymi (w) z bazy danych są przekazywane do dekodera.
4. Secret Extraction Code (SEC) przechowywany pod kluczem w jest stosowany do uzyskania sekretu (v) z danych podanych przez użytkownika (y^n) - $\mathbf{v=i}$ jeżeli $\mathbf{y^n \in D_i}$
5. jeżeli F (v) = F (s), uwierzytelnianie przebiegło pomyślnie.