Document de Fonaments

Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i Comunicació

Cristian Requena Barreda

INTRODUCCIÓ

Tot just durant els últims anys, l'autenticació d'usuaris mitjançant les seves característiques biomètriques ha començat a adinsar-se al *mainstream*, és a dir, ha guanyat popularitat, s'ha estès el seu ús i, en definitiva, ha acabat sent rellevant.

Molts dels seus usos comencen a ser quotidians, amb màquines de fitxatge de presència per empremta digital, desbloqueig d'accessos mitjançant l'escaneig de l'iris, i, des de fa uns mesos, fins i tot al palmell de la mà – els telèfons mòbils tot just comencen a incorporar autenticació biomètrica.

Seguint la tendència de l'estat de l'art d'aquesta àrea de coneixement de la seguretat de la informació, aquest treball final de màster se centra en l'anàlisi i desenvolupament d'una eina informàtica que permeti dur a terme l'autenticació d'usuaris mitjançant les característiques biomètriques de la veu.

Durant la primera fase d'aquest treball s'ha realitzat una cerca metòdica per estudiar la situació actual en l'ús de la veu com eina d'autenticació, que s'explica en més profunditat al punt corresponent.

En una segona fase, es desenvoluparà l'eina descrita anteriorment. Com es tractarà d'un període de desenvolupament d'uns dos mesos, s'ha creat una planificació de treball per a definir el conjunt de fites que seran assolides.

RECERCA BIBLIOGRÀFICA

Durant la fase de recerca s'ha localitzat un ampli conjunt de papers descrivint diversos mètodes per generar claus criptogràfiques a partir de les característiques biomètriques d'un individu. D'aquests, s'han triat quatre de representatius i rellevants, que es relacionen a continuació.

Títol	**Autor/s**	**Data i tipus de publicació**
Cryptographic Key Generation from Voice [1]	Fabian Monrose, Michael K. Reiter, Qi Li, Susanne Wetzel	2001, conferència IEEE.
Biometrics-based cryptographic key generation	Yao-Jen Chang, Wende Zhang, Tsuhan Chen	2004, conferència IEEE.
Multi-speaker voice cryptographic key generation	L. Paola Garcia-Perera, J. Carlos Mex-Perera, Juan A. Nolazco-Flores	2005, conferència IEEE.
You are the Key: Generating Cryptographic Keys from Voice Biometrics	Brent Carrara, Carlisle Adams	2010, conferència IEEE.

D'altra banda, s'ha localitzat un producte comercial[1] que permet la realització de l'autenticació d'usuaris mitjançant la veu.

1 http://www.nuance.com/landing-pages/products/voicebiometrics/

METODOLOGIA

L'eina serà desenvolupada i executada a un entorn Linux, tot i que es farà un especial èmfasi en que el codi sigui portable a altres plataformes. Per tant, s'evitarà al màxim possible les capes d'entrada i sortida de baix nivell, pel que s'empraran biblioteques portables en la mesura del possible.

D'entre les opcions per a realitzar el tractament del sistema d'entrada i sortida d'àudio d'un computador, s'ha triat una biblioteca anomenada OpenAL, ja que té diverses característiques que la fan interessant:

1. Tractament d'entrada d'àudio a baix nivell.
2. Cross-platform tant per PC (Windows i Linux) com per mòbil (Android, iOS, BlackBerry).
3. Versions de codi obert, tot i que les darreres són propietàries.

No es considera que la decisió del llenguatge de programació a emprar sigui rellevant, ja que la biblioteca OpenAL disposa de múltiples *wrappers* per molts llenguatges.

PLANIFICACIÓ

El període complet per dur a terme les tasques de desenvolupament de l'eina és de dos mesos, que han estat dividits en un conjunt de fites a assolir:

- Fita 1: Configuració de l'entorn i proves.
  Caldrà obtenir la biblioteca OpenAL i enllaçar-la a l'eina de desenvolupament triada, per tal de poder accedir a l'entrada d'àudio del sistema.
  És convenient fer proves i detectar els possibles problemes o incompatibilitats, amb l'objectiu de, si és necessari, poder reaccionar i substituir la biblioteca.

- Fita 2: Mètode d'entrada bàsic.
  Sota petició de l'usuari, realitzar la gravació d'àudio durant un lapse de temps fix, i realitzar operacions bàsiques sobre el mateix; per exemple, la detecció del soroll de fons.

- Fita 3: Mètode d'entrada intel·ligent.
  Millorar el codi desenvolupat per la fita 2 i, en comptes d'establir un límit temporal, detectar quan l'usuari comença i acaba de parlar, per tal d'enregistrar l'àudio durant el temps requerit.

- Fita 4: Realització d'operacions bàsiques.
  Sobre l'àudio obtingut amb el mètode d'entrada desenvolupat per la fita 3, executar operacions bàsiques per començar a tractar les característiques de la veu. Per exemple, obtenir la freqüència màxima i mínima de la veu, i, si escau, dades estadístiques simples.

- Fita 5: Selecció de *centroids*.
  Seguint l'algorisme descrit per la referència bibliogràfica més referenciada [1], realitzar la tria dels punts centrals de l'espectre de so enregistrat a la fita 3.

- Fita 6: Autenticació a partir dels descriptors
  Implementació de l'algorisme per autenticar els usuaris.

CRONOGRAMA

Es planifica l'entrega de les diverses fites a partir del següent cronograma:

	Setmana 1	**Setmana 2**	**Setmana 3**	**Setmana 4**
Abril	Fita 1	Fita 2		Fita 3
Maig	Fita 4		Fita 5	
Juny	Fita 6			

És a dir:

- Fita 1: Diumenge, 6 d'abril de 2014.
- Fita 2: Diumenge, 13 d'abril de 2014.
- Fita 3: Diumenge, 27 d'abril de 2014.
- Fita 4: Diumenge, 4 de maig de 2014.
- Fita 5: Diumenge, 18 de maig de 2014.
- Fita 6: Diumenge, 8 de juny de 2014.

A partir de la darrera entrega, es disposarà d'un lapse de 10 dies per acabar d'elaborar la memòria del treball.