Retour d'expérience de l'atelier *Cartes à puce-Biométrie* pour les parcours *Réseaux et Sécurité* et *Informatique Embarquée*

Guillaume Renier[1], Ghiles Mostafaoui[1], Iryna Andriyanova[1]

***Abstract*— Ce papier fait le retour d'expérience sur l'atelier *Cartes à puce – Biométrie*, conçu pour des étudiants de la deuxième année du Master en informatique et ingénierie des systèmes complexes à Cergy-Pontoise. L'objectif d'atelier est la création d'un système d'authentification forte basée sur l'utilisation d'une carte à puce et la validation de données biométriques. Pour mener à bien le travail, les étudiants sont appelés de se mettre en groupes. Ceci se fait assez naturellement, vu que la première partie des étudiants (parcours *Réseaux et Sécurité*) ont des compétences en chiffrement et authentification, tandis que la deuxième partie (parcours *Intelligence Embarquée*) a plutôt de l'expérience en systèmes embarqués et traitement d'images. L'atelier reçoit des évaluations très positives de la part des étudiants.**

I. Introduction

A. Contexte

Cette communication a pour objet l'atelier *Cartes à puce – Biométrie* proposé dans le cadre des les parcours RS et IE de la formation de niveau Master "Systèmes intelligents et communicants" (SIC) à CY Cergy Paris Université (anciennement Université de Cergy-Pontoise). Le Master est systématiquement classé par Eduniversal parmi les meilleurs masters en informatique et en ingénierie des systèmes complexes. Il occupe la 4ème place dans le dernier classement, publié en 2019 [1].

Le Master SIC s'articule autour de deux années universitaires. La première année est à parcours indifférenciés (Master 1). La deuxième année (Master 2) présente un choix de 8 différents parcours, dont 3 professionnalisants (formation par alternance) et 5 en recherche (formation initiale). Les 3 parcours professionnalisants sont : *Réseaux et Sécurité (RS)*, *Informatique Embarquée (IE)* et *Systèmes Intelligents et Distribués (SID)*. Master 1 est constituée d'un tronc commun (premier semestre) et d'options spécialisantes (second semestre). Le tronc commun permet aux étudiants d'acquérir un socle de fondamentaux théoriques et techniques nécessaires à la poursuite de leurs études. Il a également pour objectif l'homogénéisation du niveau des connaissances de la promotion. Les modules d'options (second semestre) viennent compléter le tronc commun et préparer la spécialisation par parcours en Master 2.

Ainsi, en 2ème semestre du Master 1 et au 1er semestre du Master 2, les étudiants du parcours RS se familiarisent avec les modules suivants : réseaux avancés ; chiffrement et applications ; virtualisation. Quant aux étudiants du parcours IE, ils suivent les modules de systèmes de traitement d'images, d'architecture pour les systèmes embarqués et d'agents et systèmes intelligents.
Grâce au tronc commun, l'ensemble des parcours ont été initiés aux sujets suivants : probabilités et statistiques ; simulation réseau ; conception orientée objet ; intelligence artificielle ; bases de données avancées ; informatique embarquée ; traitement du signal ; traitement d'images. Il est aussi important de noter que les étudiants de tous les parcours suivent le module de gestion de projets informatiques durant toute la formation et ont donc acquis de bonnes pratiques de travail en équipe.

Le Master SIC propose également un certain nombre d'ateliers pour les parcours professionnalisant en Master 2. Le principe d'un atelier est de faire travailler les étudiants sur un sujet qui synthétise deux ou plusieurs domaines parmi ceux enseignés en Master. L'objectif final est la conception d'un logiciel ou d'un système "intelligent". Chaque atelier contient un pourcentage important d'heures de travail en autonomie. Les enseignants servent plutôt de "coaches" en faisant des interventions sur des aspects très ciblés ou pendant des moments de blocage. Le travail se fait par groupes d'étudiants. L'équipe pédagogique s'assure que l'union des compétences de chaque groupe d'étudiants recouvre l'ensemble des compétences pré-requises pour l'atelier en question.

L'atelier *Cartes à puce – Biométrie* est mis en place depuis 2014. Il est destiné aux étudiants des parcours RS et IE. L'atelier est planifié pour le début du 2ème semestre de Master 2. Il est basé sur le cours de chiffrement [2] (vu par les étudiants RS) et le cours de système de traitement d'images [3] (vu par les étudiants IE). Notons que les étudiants RS ont les connaissances de base en traitement d'images. Aussi, les étudiants IE ont des connaissances de base sur les protocoles de communication. La réussite d'un étudiant dans cet atelier est donc conditionnée par les connaissances techniques de son métier principal, mais aussi par un travail collaboratif cohérent à l'intérieur de son groupe.

Dans les sections suivantes nous faisons un retour d'expérience pédagogique sur la mise en place de l'atelier *Cartes à puce – Biométrie*. Après avoir formulé les objectifs de l'atelier, nous présentons son déroulement et sa maquette pédagogique suivis par le retour donné par nos étudiants.

[1]Département des Sciences Informatiques, Laboratoire ETIS UMR 8051, CY Cergy Paris Universite, 95015 Cergy-Pontoise, France. E-mail : *prenom.nom@u-cergy.fr*

B. Objectifs de l'atelier

Le but de l'atelier *Cartes à puce-Biométrie* est de monter un système d'authentification forte cohérent avec un contexte de service de biométrie. Les étudiants doivent proposer un schéma d'authentification reposant sur deux éléments :

1) Un challenge lié à la connaissance d'un couple `login/mot de passe`. Les étudiants vont donc, sur ce point, définir le processus de challenge (côté client et serveur). Ils sont amenés à réfléchir et à définir le protocole de vérification. Enfin ils doivent trouver leur manière de stocker les mots de passe.
2) Un challenge lié à la possession d'une carte à puce. Pour ce challenge ils prennent en charge l'écriture d'un programme de lecture/écriture d'une carte à puce (`Python` ou `Java`). Ce point est lié à la partie biométrie.

Le schéma d'authentification est à inventer. Les étudiants seront invités à justifier la pertinence de leurs choix et démontrer qu'ils ont fait une étude de sécurité (recherche de failles de sécurité, de moyens de contournement) et proposer des contres-mesures. Le processus d'authentification se faisant dans un certain contexte, les contres-mesures seront jugées par leur cohérence : est-ce que le poste client d'authentification est sûr ? contrôlé ? etc.

II. Déroulement de l'atelier

Cette section détaille le déroulement de l'atelier.

Mise en place de l'atelier et son calendrier

L'équipe pédagogique est composée de deux personnes : un expert en sécurité informatique (Guillaume Renier) et un expert en traitement d'images (Ghiles Mostafaoui). Quant aux étudiants, ils se regroupent en équipes de 3-4 personnes en veillant à la bonne composition d'équipe : chaque équipe doit contenir au moins un étudiant RS et un étudiant IE. Ceci permet de s'assurer que l'équipe est capable de travailler sur l'atelier en autonomie indépendamment des autres groupes et des enseignants.

Un lecteur de cartes et 4-5 cartes sont mis à disposition de chaque équipe. Les lecteurs de cartes sont reconnus automatiquement par les ordinateurs `Windows` et `MacOS`, et nécessitent l'installation de la librairie `libccid` pour les utilisateurs `Linux`. il est possible de déplacer les lecteurs. Les cartes à puce mises à disposition sont de simples cartes de stockage, de 170 octets de volume (donc elles ne sont pas protégées ni contre la copie ni contre aucun type d'attaque). Les spécifications des cartes et des lecteurs sont fournies.

L'atelier dure 5 jours (10 demi-journées), du lundi matin au vendredi soir. Le déroulement est comme suit :

A. **Lundi matin :** cours d'une demi-journée sur la notion d'authentification.
B. **Lundi après-midi :** cours d'une demi-journée présentant une méthode d'authentification biométrique reposant sur la détection de visage et la reconnaissance de l'iris.
C. 7 **demi-journées** de travaux pratiques.
D. **Vendredi après-midi :** soutenance et démonstration du système biométrique mis en place suivies par le debrieffing avec les enseignants.

A. Cours sur l'authentification

L'intervention de l'enseignant en sécurité informatique permet de repenser les notions d'authentification dans le contexte d'une application spécifique. Le cours détaille les techniques à mettre en oeuvre pour déterminer la validité d'une authentification (notion de challenge), pour stocker les informations d'authentification (mot de passe), pour éviter les attaques par rejeu. Il est divisé en quatre parties, détaillées ci-dessous.

Attaques par rejeu. Ici, on étudie le cas d'envoi d'un mot de passe (souvent en clair) dans un tunnel `SSH`. L'idée est d'étudier les faiblesses d'un tel système (essentiellement attaque au niveau serveur pour récupération des mots de passe en clair) et de voir comment améliorer ce système pour éviter les attaques par rejeu interne (rejeu d'un processus d'authentification pour le même service) ou externe (rejeu du processus avec des informations obtenues pour une authentification dans un autre système).

Authentification. L'objectif de cette partie est d'expliquer que le mot de passe en clair ne soit jamais ni connu du serveur d'authentification, ni envoyé sur le réseau. L'utilisation d'une fonction de hachage est préconisée, avec la mise en place des challenges (avec "sel" dans le stockage et "graine" dans l'envoi). Les protocoles de hachage présentés sont `MD5` et `SHA1` en insistant sur le fait qu'elles sont obsolètes mais que pour un usage web dans un contexte non sensible, l'utilisation des ces fonctions dans un schéma `HMAC` ou `PBKDF` peut-être suffisant si le terminal ou l'implémentation ne permet pas d'utiliser un protocole de type `SHA`. La notion d'authentification forte [1] et faible est présentée, aussi que la notion de challenge et les preuves Zero-Knowledge (ZK). Cette partie du cours sert de rappel aux étudiants RS et permet d'identifier rapidement des protocoles d'authentification à utiliser dans le cadre de l'atelier (important pour les étudiants IE).

Cartes à puce. L'objectif ici est surtout d'apporter les notions de base sur les cartes à puce (types de cartes, cartes avec et sans contact, différence technologique et/ou de logiciel, protocoles d'anti-collision pour les cartes sans contact), qui permettent de commencer à développer rapidement. Suite à cette partie, les étudiants

1. Dans le cadre de l'atelier, une authentification est dite forte lorsqu'elle met en oeuvre au moins 2 des 3 possibilités parmi : (a) authentification à l'aide d'un mot de passe, (b) utilisation d'une carte à puce et d'un code `PIN`; (c) détection biométrique d'utilisateur.

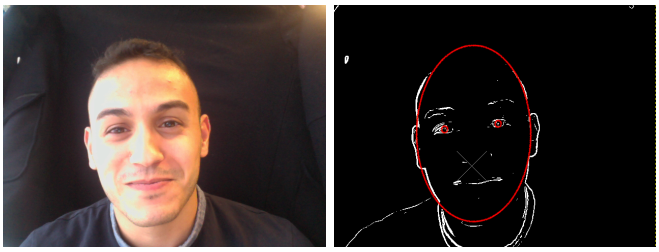

Fig. 1. Une capture de camera (à gauche) et une image traitée (à droite), utilisée ensuite pour la détection du visage et des yeux.

sont capables de stocker, lire des données et valider une authentification (vérifier que le code `PIN` est bon).

Définition d'un schéma d'authentification complet. Le cours est terminé par la présentation d'un schéma très général intégrant la carte à puce, l'utilisation d'un mot de passe et de la biométrie. L'enseignant a pour consigne de ne pas présenter le schéma tout prêt à déployer, car ceci rentre dans le cadre du travail en autonomie. Finalement, la mise en place de l'analyse de sécurité est discutée : comment cherche-t-on des failles et quelles contre-mesures pourraient être effectués.

B. Cours sur la biométrie

L'intervention d'un expert en traitement d'images permet d'initier les étudiants , dans le cadre très appliqué de cet atelier, à certains algorithmes de base de traitement d'images qui peuvent être utilisés pour la biométrie. Les étudiants s'appuient sur les connaissances en traitement d'images acquises en Master 1 et dans les deux ateliers précédents celui-ci (indexation d'images et traitement d'images temps réel). L'objectif ici est de pouvoir aller un peu plus loin sur les aspects de reconnaissance de formes temps réel.

Un focus particulier est fait sur la détection de visage et la détection de l'iris des yeux à l'aide d'une transformée de Hough généralisée [4] (détection d'ellipse pour le visage et de cercle pour l'iris). La reconnaissance de l'iris est ensuite abordée par l'utilisation de descripteurs très simples permettant de caractériser la couleur et la texture d'iris.

Le cours contient deux parties : la reconnaissance de formes et la mise en place de signatures biométriques.

Reconnaissance de formes et son application à la détection du visage/des yeux La Transformée de Hough Généralisée (THG) est introduite et son implémentation temps réel, à l'aide de Lookup Tables (LUT) est discutée.On considère ensuite l'application de l'algorithme THG pour à la fois la détection d'une ellipse pour le visage et celle de deux cercles les iris des yeux (voir Fig.1 pour illustration).

Signature biométrique L'objectif ici est de définir les caractéristiques "image" de l'iris à utiliser comme signature biométrique et discuter de leur utilisation en tenant compte de l'aspect temps réel et des contraintes physiques du système (notamment, la mémoire disponible sur la carte à puces). On compare les caractéristiques diverses de l'iris (couleur, histogrammes, texture) pour en déduire un critère de sélection pertinent et utilisable permettant de les identifier.

C. Travaux pratiques

Pendant les travaux pratiques, les équipes d'étudiants implémentent un système biométrique dans lequel l'utilisateur : (a) insère sa carte dans le lecteur ; (b) saisit son code PIN/mot de passe ; (c) se fait photographier par la caméra. Suite à cela le système authentifie l'utilisateur.

Chaque équipe est libre de choisir un langage de programmation mais il est conseillé d'utiliser `Java6`. Les protocoles `MD5` et `SHA1` sont faciles à implémenter en `JavaScript`. La carte à puce utilisée suit la spécification `GEMALTO MEM CLUB v2`, ce qui définit les processus de lecture/écriture des données binaires de/vers la carte.

Les étudiants ont comme consigne de sauvegarder l'*empreinte* de chaque utilisateur, autrement dit son identifiant (`login`), des données d'authentification et des données biométriques. Nous insistons sur le fait qu'ils choisissent eux-mêmes la méthode en se basant sur les deux cours au début de l'atelier. Dans la phase finale, ils doivent justifier leur choix (la solution est-elle implémentable sur l'équipement fourni ? Le niveau de sécurité est-il suffisant ?). Par exemple, si l'empreinte biométrique est sauvegardée sur la carte à puce, il faut justifier si son volume ne dépasse pas le volume de mémoire de la carte. Donc, il va falloir choisir avec parcimonie la caractéristique qui donne la signature biométrique de chacun. Une approche possible serait, par exemple, d'utiliser l'histogramme couleur de l'iris.

Pendant la phase des travaux pratiques, les enseignants se trouvent sur le campus de l'université. Ils sont disponibles en temps réel par e-mail ou par visioconférence, et se déplacent dans la salle Master s'il y a un blocage. Chaque équipe a une réunion avec un enseignants lors de la 4è demi-journée, afin de valider les contextes et les schémas d'authentification proposés.

D. Evaluation des étudiants et clôture de l'atelier

Vendredi, avant les soutenances, les étudiants déposent un rapport par équipe, succinct (5 pages), décrivant le dispositif, ses fonctionnalités et l'organisation de l'équipe.

Vendredi après-midi est donc réservée aux démonstrations et soutenances.

La démonstration dure 20 minutes par équipe. Elle doit contenir les scénarios d'usage suivants : (a) authentification d'utilisateur sincère, (b) authentification d'utilisateur qui a oublié son mot de passe, (c) tentatives de fraudes (notamment avec la carte valide, avec une copie de la carte, avec les bons identifiants mais sans carte). Les étudiants doivent présenter l'analyse de sécurité de leur solution développée et proposer d'éventuelles contres-mesures pour les failles existantes.

La démonstration est suivie par une séance de questions-réponses qui clôture la soutenance.

L'évaluation de la soutenance est basée sur plusieurs critères :

— Gestion de la parole, partage de la parole,
— Qualité du support de présentation,
— Déroulement du scénario de la démo,
— Présentation du contexte d'utilisation, pertinence et cohérence du schéma d'authentification proposé,
— Pertinence et cohérence de l'utilisation de la carte à puce,
— Implémentation technique de la méthode d'authentification, gestion des mots de passe,
— Implémentation technique de la méthode de détection et de reconnaissance de formes pour la biométrique,
— Justesse des explications liées au fonctionnement de la méthode biométrique,
— Enfin : analyse des erreurs, recul sur les problèmes de programmation.

A la fin des soutenances, les enseignants font un debrieffing avec les étudiants : un avis plus global est donné sur le travail et la manière de présenter les résultats. Les enseignants conseillent éventuellement sur la manière de présenter, le vocabulaire utilisé et la gestion du temps de parole. L'objectif est de préparer les étudiants à la présentation d'un produit de sécurité.

III. Compétences acquises et évaluation de l'atelier

Notre atelier permet de s'assurer que les étudiants RS et IE ont acquis les **compétences suivantes** :

(a) Assemblage du dispositif complet (cartes à puces, caméras, liaison avec l'ordinateur).
(b) Etablissement de la communication entre l'ordinateur et la carte à puce (lecture/écriture).
(c) Acquisition du flux d'image (gestion de l'acquisition, de l'affichage, et traitements de base sur les images).
(d) Réalisation d'un algorithme de détection de formes afin de détecter puis caractériser l'IRIS.
(e) Déduction de l'empreinte biométrique en rapport avec les capacités de la carte à puce.
(f) Mise en oeuvre d'un prototype : préparation de la carte à puce, configuration de l'application.
(g) Authentification de l'utilisateur.
(h) Mise en place d'une démonstration : utilisateur sincère, utilisateur qui oublie son mot de passe, tentatives de fraudes (avec la carte, avec une copie de la carte, avec les bons identifiants...)
(i) Cryptanalyse du système d'authentification mis en place en fonction de la compromission des différents éléments mis en jeu : soit une étude théorique, soit une mise en pratique.
(j) Proposition de contres-mesures.

L'**évaluation** de l'atelier par des étudiants s'effectue d'une manière anonyme via un GoogleForms, la forme de l'évaluation étant commune à tous les cours du Master. Les critères d'évaluation sont les suivants : clarté de l'énoncé et définition explicite des objectifs de l'atelier ; la cohérence de la quantité de travail demandée par rapport au nombre d'heures allouées ; la qualité des cours et des supports des cours ; qualité des interactions avec l'équipe pédagogique ; indication des points forts et des points faibles de l'atelier.

Voici quelques indicateurs concernant l'édition 2020 de l'atelier. A ce jour (2 semaines après la fin d'atelier), 40% d'étudiants ont rempli la fiche d'évaluation. 100% des évaluations sont très positifs (des notes $4-5$ sur 5 sur tous les critères). Parmi les points forts les étudiants citent le côté applicatif de l'atelier. Parmi les points faibles – la précision plutôt faible de la méthode de reconnaissance d'iris. Cette critique est par ailleurs justifiée. En effet, les contraintes de temps (nombre d'heures de travail disponibles), d'exécution temps réel ainsi que les limites physiques du système obligent à considérer des méthodes de reconnaissance d'iris très simples et peu couteuses et de ce fait aux performances limitées.

IV. Discussion

L'atelier *Cartes à puce-Biométrie* a beaucoup du succès auprès des étudiants Master en parcours RS et IE. Les étudiants apprécient le fait que l'atelier soit crée autours des notions d'actualité (authentification par hachage et sécurité informatique en général, et authentification biométrique). Le fait de travailler sur les cartes à puces très basiques est considéré comme un atout supplémentaire, car cela permet de réfléchir sur la complexité de la mise en oeuvre d'un système biométrique. La partie d'authentification utilise les protocoles de hachage simples, ce qui permet de proposer cet atelier aux Étudiants qui n'ont pas eu un cours de chiffrement.

Une difficulté principale de cet atelier est la fiabilité peu élevée de la reconnaissance de l'iris et la sensibilité des algorithmes de traitement d'image (THG, détection du visage et de l'iris) aux changement de luminosité de la pièce, au type de caméra etc.

La question du choix du support matériel peut également être posée. L'avantage de la carte à puces actuelle est sa simplicité d'utilisation, ce qui est important pour un atelier assez chronophage. Dans le futur, on souhaite proposer l'utilisation de `crypto card`, avec plus de fonctionnalités. Il reste à vérifier si le travail préliminaire sur la programmation de ce type de cartes s'inscrit bien dans le cadre de l'atelier de 5 jours.

References

[1] Eduniversal, "TOP 10 2019 - Classement Master Informatique et Ingénierie des Systèmes."
[2] L. R. Knudsen, *Cryptology - How to crack it*, 2017.
[3] C. Achard, *Cours de Traitement d'images*, 2003.
[4] R. O. Duda and P. E. Hart, "Use of the Hough transformation to detect lines and curves in pictures," *Commun. ACM*, vol. 15, no. 1, p. 11–15, Jan. 1972.