الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
-البويرة-

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥağ - Tubirett -

جامعة البويرة

كلية العلوم والعلوم التطبيقية
Faculté des Sciences et des Sciences Appliquées

المرجع:...../م م/ 2021
Référence : ...../MM/2021

Mémoire de Master

Présenté au

Département : Génie Électrique
Domaine : Sciences et Technologies
Filière : Electronique
Spécialité : Electronique des systèmes embarqués

Réalisé par :

LAREF AFAF

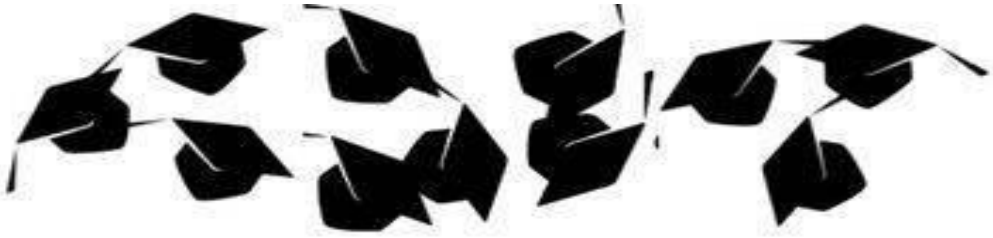
Thème

Résolution des problèmes de sécurité dans les systèmes embarqués

Soutenu le: 03/07/2023

Devant le Jury composé de :

Mr : BEN SAFIA	M.C.A	Univ. Bouira	Président
Mr : TOUAFEK	M.A.A	Univ. Bouira	Rapporteur
Mr : BOUGHAROUAT	M.C.A	Univ. Bouira	Examinateur



Dédicace

À mes très chers parents, qui ont toujours été présents pour moi et m'ont donné un magnifique exemple de travail acharné et de persévérance. J'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour.

À mes chers frères : Mahmoud, Salim, Khaled, Mourad et Amine. Vous avez été des compagnons de vie précieux et je suis reconnaissante de vous avoir à mes côtés. Votre soutien inconditionnel a été une source d'inspiration pour moi.

À ma famille adorable, que Dieu la protège. Votre amour et votre soutien constant ont été les piliers de ma réussite. Je vous suis profondément reconnaissante pour tout ce que vous avez fait pour moi.

À tous les enseignants qui ont croisé ma route au cours de ces années d'études, je vous adresse mes sincères remerciements. Votre dévouement et votre savoir m'ont permis de grandir et de me développer académiquement.

À mes chères amies Lilya, Ouardia, Mounia et Yousra, vous avez été des compagnes précieuses tout au long de cette aventure. Votre soutien, votre amitié et vos encouragements m'ont aidé à surmonter les défis. Je vous suis reconnaissante pour votre présence.

Et à mes amis Azzedine, Ismail et abdellah je tiens à exprimer ma gratitude pour votre amitié sincère. Vos encouragements et votre soutien moral ont été d'une valeur inestimable.

Je suis reconnaissante envers chacune des personnes mentionnées

et je les remercie du fond du cœur pour leur soutien indéfectible

Tout au long de mon parcours.

LAREF AFAF

Remerciements

Je tiens tout d'abord à exprimer ma gratitude envers Dieu le Tout-Puissant qui m'a accordé la volonté et le courage nécessaires pour mener à bien ce travail.

Je souhaite également exprimer ma profonde reconnaissance envers ma famille pour son soutien moral. Sa présence et son encouragement constants ont été essentiels dans la réalisation de ce projet. Ce travail témoigne de ma gratitude envers elle.

Je tiens à adresser mes sincères remerciements à mon promoteur Mr. Yaakoub Touafek, qui m'a accompagné dès le début de ce projet et tout au long de ma formation. Sa guidance et ses conseils précieux ont été d'une importance capitale.

J'exprime également ma gratitude envers l'ensemble de mes professeurs qui ont contribué à mon parcours universitaire au sein de l'Université de Bouira. Leur soutien indéfectible et leur accueil chaleureux ont été une source d'inspiration pour moi.

Je tiens à remercier également les membres du jury pour avoir accepté d'évaluer ce travail. Leur expertise et leurs commentaires constructifs ont grandement enrichi mon travail. Je leur suis reconnaissant pour toutes les raisons qui les ont amenés à participer à cette évaluation.

Enfin, je souhaite exprimer ma gratitude à toutes les personnes qui ont contribué de près ou de loin à la réussite de ce modeste travail. Leurs conseils, leur encouragement et leur soutien ont été précieux et ont largement contribué à mon succès.

Encore une fois, je remercie sincèrement toutes les personnes

Mentionnées ci-dessus pour leur soutien inestimable.

LAREF AFAF

Résumé

Résumé

Notre mémoire se concentre sur la sécurité des systèmes embarqués, en se focalisant sur la carte Mifare Classique 1k. Le premier chapitre de ce mémoire aborde les généralités des systèmes embarqués et leurs problèmes de sécurité. Il met en évidence les défis auxquels sont confrontés ces systèmes en termes de vulnérabilités et d'attaques potentielles.

Le deuxième chapitre se concentre sur la carte à puce en tant que composant clé des systèmes embarqués. Il explique son fonctionnement et son utilisation dans différents domaines, tout en soulignant les risques de sécurité associés à cette technologie.

Le troisième chapitre présente une solution de sécurité pour la carte à puce en utilisant le chiffrement, les protocoles d'authentification et les contrôles d'accès. Une méthodologie de chiffrement détaillée est proposée, suivie d'une évaluation expérimentale. Les résultats démontrent les améliorations de sécurité apportées par cette solution. De plus, une double vérification avec clavier, clé mécanique, carte Arduino et RFID est proposée pour contrer les attaques physiques. Cette approche renforce la sécurité en ajoutant une couche supplémentaire de vérification. Ainsi, la solution offre une protection contre les attaques physiques et améliore la sécurité des systèmes embarqués.

Mots clés : Systèmes embarqués, Sécurité, Problèmes de sécurité, Vulnérabilités, Piratage

Attaques physiques, Défauts de conception, Confidentialité des données.

الملخص

مشروع تخرجنا يركز على أمان الأنظمة المضمنة، مع التركيز على بطاقة ميفار الكلاسيك

يتناول الفصل الأول من هذا المشروع العمليات المتعلقة بالأنظمة المضمنة ومشاكل أمانها. يسلط الضوء على التحديات التي تواجه هذه الأنظمة من حيث الثغرات والهجمات المحتملة.

يتركز الفصل الثاني على بطاقة الشريحة كمكون رئيسي للأنظمة المضمنة. يشرح عملها واستخدامها في مجالات مختلفة، مع التركيز على المخاطر الأمنية المرتبطة بهذه التكنولوجيا.

يقدم الفصل الثالث حلاً أمنيًا لبطاقة الشريحة باستخدام التشفير وبروتوكولات المصادقة وضوابط الوصول. يتم تقديم منهجية تفصيلية للتشفير، تليها تقييم تجريبي. تظهر النتائج تحسينات في الأمان التي يوفرها هذا الحل. بالإضافة إلى ذلك، يتم اقتراح التحقق المزدوج باستخدام لوحة مفاتيح ومفتاح ميكانيكي وبطاقة أردوينو و RFID لمواجهة الهجمات المادية. تعزز هذه النهج الأمان من خلال إضافة طبقة إضافية من التحقق. بالتالي، يوفر الحل حماية ضد الهجمات المادية ويعزز أمان الأنظمة المضمنة.

Abstract

Our thesis focuses on the security of embedded systems, specifically on the Mifare Classic 1k card. The first chapter of this thesis addresses the general aspects of embedded systems and their security issues. It highlights the challenges faced by these systems in terms of vulnerabilities and potential attacks.

The second chapter concentrates on the smart card as a key component of embedded systems. It explains its functioning and usage in various domains, while emphasizing the security risks associated with this technology.

The third chapter presents a security solution for the smart card by utilizing encryption, authentication protocols, and access controls. A detailed encryption methodology is proposed, followed by an experimental evaluation. The results demonstrate the security enhancements brought about by this solution. Furthermore, a dual verification approach using a keypad, mechanical key, Arduino board, and RFID is suggested to counter physical attacks. This approach strengthens security by adding an additional layer of verification. Thus, the solution provides protection against physical attacks and enhances the security of embedded systems.

.

Table de matières

Liste des figures ……I.

Liste des tableaux ……II.

Liste des acronymes ……III.

Introduction Générale ……IV.

Chapitre 1 : Généralité sur les systèmes embarqués et leurs problèmes de sécurité

1 Introduction Générale 1

1 Introduction : 3

1.1 Présentation de systèmes embarqués : 3

2 L'importance des systèmes embarqués dans notre vie quotidienne : 4

3 Caractéristiques principales d'un système embarqué : 5

4 L'architecteur d'un système embarqué : 5

5 Les compositions d'un système embarqué : 6

6 L'art de bien concevoir un système embarqué : 9

7 Domaine d'application des systèmes : 10

8 Problèmes de sécurité dans les systèmes embarqués : 11

8.1 Concepts de base de la sécurité : 11

8.1.1 La confidentialité : 11

8.1.2 L'intégrité : 11

8.1.3 La disponibilité : 12

9 Les attaques dans les systèmes embarqués : 12

9.1 Sources d'attaques dans les systèmes embarqués : 12

9.2 Utilisation de clés de cryptographie faibles : 12

9.3 Réutilisation de codes et de composants non sécurisés : 12

10 Types d'attaque : 12

11 Classification des attaques : 13

11.1 Critère 1 : L'objectif fonctionnel : 13

11.2 Critère 2 : les méthodes utilisées : 14

Chapitre 2 : Carte à puce

12 Conclusion : 15

1 Introduction : 16

1.1 Présentation de la carte à puce 16

1.2 Composants essentiels d'une carte à puce : 17

2 Familles et types de cartes : 18
2.1 Familles de carte à puce : 18
2.2 Types de cartes : 18
3 Présentation de la technologie RFID : 19
3.1 Que sont les cartes RFID ? 19
3.2 Les catégories de puces RFID : 19
4 Les familles de puces RFID 20
5 Constitutifs d'un système RFID : 21
6 Comment fonctionnent les cartes d'accès RFID : 21
7 Comment le système communique ? 22
8 Classification des cartes RFID basée sur la longueur d'onde de fréquence de la puce RFID 23
8.1 Cartes RFID basse fréquence (LF) 23
8.2 Cartes RFID haute fréquence 23
8.3 Cartes RFID à ultra-haute fréquence (UHF) : 23
9 Description détaillée des composants des cartes RFID 23
10 Présentation de la carte à puce RFID Mifare Classic 1K: 25
11 Les types d'attaque de la carte RFID : 25
12 Conclusion : 30

Chapitre 3 : Proposition d'une solution contre les attaques physiques avec une double vérification (clavier, clé mécanique)

1 Introduction 31
1.1 Unité de commande et de traitement 31
1.1.1 La carte Arduino UNO 31
1.1.2 Caractéristiques techniques de la carte Arduino UNO 32
2 Module RFID 33
3 L'IDE Arduino 36
4 Logiciel de simulation 37
4.1 Fritzing 37
5 Clavier numérique 4x4: (Keypad Module) 38
6 La serrure électromagnétique 12v 38
7 Circuit et composant 39
8 Les programmes de réalisations : 39
9 Résultat de réalisation : 42
10 Conclusion 43
11 Conclusion Générale : 51
12 Bibliographie 61

Liste des figures

Chapitre 1 : Généralité sur les systèmes embarqués et leurs problèmes de sécurité

Figure 1- 1 Les exemples sur les systèmes embarqués 4
Figure 1- 2: Architecture générale d'un système embarqué 6
Figure 1- 3 : Composition d'un système embarquée 7
Figure 1- 4 : Processeur 7
Figure 1- 5 : La Mémoire 8
Figure 1- 6: Le périphérique d'entrée-sortie(E/S) 8
Figure 1- 7 : Les interfaces 9
Figure 1- 8: Les logiciels embarqués 9
Figure 1- 9: Les alimentations 9
Figure 1- 10 : Domaines d'application des systèmes embarqués 11
Figure 1- 11 : Classification des attaques dans les systèmes embarqués 13
Figure 1- 12 : Classification des attaques dans les systèmes embarqués selon les méthodes utilisée [10]. 14

Chapitre 2 : Carte à puce

Figure 2- 1: Les contacts d'un module de carte à puce 17
Figure 2- 2: Schéma simplifié d'une carte à puce 18
Figure 2- 3:Carte à puce RIFD 19
Figure 2- 4 : Constitutifs d'un système RFID 21
Figure 2- 5 : Fonctionnent les cartes d'accès RFID 22
Figure 2- 6 : Composant cartes RFID 24
Figure 2- 7:Mifare card 1k 25
Figure 2- 8:Fichier dump d'une carte Mifare 26
Figure 2- 9 : Mise en situation d'un man-in-the-middle 27
Figure 2- 10 : Schéma avec oscillateur et antenne 27

Chapitre 3 : Proposition d'une solution contre les attaques physiques avec une double vérification (clavier, clé mécanique)

Figure 3- 1 : La carte arduino UNO 31
Figure 3- 2 :Les E/S d'une carte arduino UNO 32
Figure 3- 3:Anatomie d'une carte Arduino UNO 33
Figure 3- 4 : Module RFID RC522 33
Figure 3- 5:Carte Mifare classic 1k 33
Figure 3- 6 : Module RFID MFRC522 34
Figure 3- 7:Brochage avec Arduino UNO. [31] 35
Figure 3- 8 : Logiciel arduino IDE 36
Figure 3- 9:Page d'accueil du logiciel Fritzing. [28] 37
Figure 3- 10 :4x4 Key pad Module 38
Figure 3- 11: Serrure électromagnétique 12v 38
Figure 3- 12:Le schéma général de notre système 39

Liste des tableaux

Tableau 3.1:Brochage avec Arduino UNO. [25] 35

Liste des acronymes

IHM	interface homme–machine
ASIC	Circuit intégré spécifique à une application
SE	System embarquées
DSP	Digital Signal Processors
CPU	Unité Centrale de Traitement
RFID	Radio Frequency Identification
LCD	Liquid Crystal Display
USB	Universal Serial Bus
UHF	Ultra High Frequency
LF	Low Frequency

Introduction Générale

1 Introduction Générale

Les systèmes embarqués jouent un rôle de plus en plus crucial dans notre vie quotidienne. Ils sont présents dans une multitude d'applications, allant des dispositifs électroniques portables aux véhicules intelligents et aux infrastructures critiques. Cependant, avec leur omniprésence croissante, les problèmes de sécurité associés à ces systèmes ont également pris de l'ampleur. Dans ce mémoire, nous nous intéressons spécifiquement aux problèmes de sécurité dans les systèmes embarqués, en mettant l'accent sur les attaques physiques et les solutions de protection.

Le premier chapitre de ce mémoire pose les bases en fournissant une introduction générale aux systèmes embarqués et en mettant en évidence leur importance dans notre vie quotidienne. Nous examinons les caractéristiques principales des systèmes embarqués, leur architecture et leurs différentes compositions. Ensuite, nous explorons les concepts de base de la sécurité, tels que la confidentialité, l'intégrité et la disponibilité, ainsi que les attaques couramment rencontrées dans les systèmes embarqués.

Le deuxième chapitre se concentre sur la carte à puce, un composant essentiel des systèmes embarqués. Nous commençons par présenter la carte à puce et ses composants essentiels. Ensuite, nous examinons les différentes familles et types de cartes à puce, en mettant également l'accent sur la technologie RFID (Radio Frequency Identification). Nous explorons les catégories de puces RFID et discutons des composants spécifiques des cartes RFID. Nous nous intéressons en particulier à la carte à puce RFID Mifare Classic 1K et examinons les types d'attaques auxquels elle est sujette.

Le troisième chapitre propose une solution pour contrer les attaques physiques sur les cartes à puce, en introduisant une double vérification basée sur un clavier numérique et une clé mécanique. Nous détaillons les composants de cette solution, notamment l'unité de commande et de traitement utilisant la carte Arduino UNO, le module RFID, le clavier numérique 4x4, la serrure électromagnétique 12v, ainsi que les circuits et les logiciels de simulation utilisés. Nous présentons également les programmes de réalisation.

En conclusion, ce mémoire met en évidence les problèmes de sécurité dans les systèmes embarqués, en se concentrant sur les attaques physiques et en proposant une solution de protection basée sur une double vérification. Cette solution offre une approche pratique pour renforcer la

sécurité des cartes à puce. En étudiant ces concepts, nous contribuons à une meilleure compréhension des défis de sécurité dans les systèmes embarqués et proposons des mesures pour améliorer leur résilience face aux attaques physiques.

En résumé, notre mémoire se concentre sur les problèmes de sécurité dans les systèmes embarqués, en mettant l'accent sur la carte Mifare Classique 1k. Nous explorons les problèmes de sécurité dans les systèmes embarqués de manière générale, en identifiant les vulnérabilités courantes. Nous proposons également une solution de sécurité pour renforcer la sécurité de la carte Mifare Classique 1k, en évaluant son efficacité par rapport aux approches existantes. Cette recherche vise à contribuer à l'amélioration de la sécurité des systèmes embarqués, en particulier ceux utilisant la carte Mifare Classique 1k.

Chapitre 1 :

Généralité sur les systèmes embarqués et leurs problèmes de sécurité

Chapitre 1 : Généralité sur les systèmes embarqués et leurs problèmes de sécurité

1 Introduction :

Les systèmes embarqués jouent un rôle prépondérant dans notre vie quotidienne, bien que nous ne soyons pas toujours conscients de leur présence. De nos téléphones intelligents aux voitures connectées en passant par les appareils ménagers, les systèmes embarqués sont omniprésents et constituent le cœur technologique de nombreux produits.

Ce chapitre vise à fournir une introduction aux systèmes embarqués, en mettant l'accent sur leurs généralités et les problématiques qui leur sont associées. Nous explorerons les principales caractéristiques de ces systèmes, leurs applications diverses et les défis auxquels ils sont confrontés.

1.1 Présentation de systèmes embarqués :

Définition :

On peut définir un système embarqué comme un système électronique et informatique autonome conçu pour accomplir une tâche spécifique. Contrairement aux dispositifs classiques, il ne possède généralement pas de périphériques d'entrée/sortie standard tels qu'un clavier ou un écran d'ordinateur. Le matériel et l'application sont étroitement liés, avec le logiciel embarqué intégré profondément dans le matériel lui-même. Dans un environnement embarqué, la frontière entre le matériel et le logiciel n'est pas aussi clairement définie que dans un environnement informatique classique tel qu'un ordinateur personnel. On retrouve des systèmes embarqués dans diverses applications, telles que les dispositifs médicaux, les véhicules, les avions, les robots industriels, les équipements de télécommunication, et bien d'autres. [1]

Ils jouent un rôle essentiel dans le fonctionnement des appareils modernes, offrant des performances précises et fiables, même dans des environnements complexes et exigeants.

Figure 1- 1 Les exemples sur les systèmes embarqués

2 L'importance des systèmes embarqués dans notre vie quotidienne :

Qu'est-ce qu'un système embarqué?

Il suffit d'observer notre environnement quotidien pour constater la présence évidente des systèmes embarqués. Dès le matin, votre réveille-matin vous tire de votre sommeil :

Un exemple de système embarqué :

- Vous programmez ensuite votre machine à café pour vous préparer un délicieux café serré encore un système embarqué.
- En allumant votre télévision et en utilisant votre télécommande, vous interagissez avec des systèmes embarqués.
- Dans votre voiture, le calculateur vocal vous rappelle de mettre votre ceinture de sécurité : un autre système embarqué.
- Vous appelez votre ami avec votre téléphone portable pour lui annoncer votre retard : encore un système embarqué.

La liste des systèmes embarqués que nous croisons sans le savoir au cours d'une journée est encore longue.

En somme, les systèmes embarqués nous entourent et nous sommes littéralement immergés dans leur présence, fidèle et prête à nous rendre service. Leur omniprésence est indéniable et ne fera que s'accroître. En réalité, nous parlons d'informatique et d'électronique. Les systèmes embarqués sont composés d'électronique plus ou moins complexe et d'informatique plus ou moins avancée. Tentons maintenant de donner une définition plus précise d'un système embarqué

Qu'est-ce que l'embarqué ?

Le terme "embarqué" peut englober plusieurs notions selon le contexte :

- ✓ Il peut faire référence au marché des systèmes embarqués, qui concerne le développement et la commercialisation de ces systèmes spécialisés.
- ✓ Il peut également être utilisé pour désigner les systèmes embarqués en tant que tels, dans un sens plus général. [2]

3 Caractéristiques principales d'un système embarqué :

Les principales caractéristiques d'un système embarqué incluent :

- Il s'agit d'un système essentiellement numérique.
- Il intègre généralement un processeur.
- Il exécute une application logicielle dédiée qui accomplit une fonction spécifique, contrairement aux applications scientifiques ou grand public traditionnelles.
- Il ne dispose pas d'un clavier standard, mais peut utiliser des boutons poussoirs, des claviers matriciels, etc. Son affichage est limité (écran LCD) voire inexistant.
- Bien qu'il ne s'agisse généralement pas d'un PC, certaines applications embarquées utilisent des architectures similaires à faible consommation d'énergie, telles que x86. Cependant, il convient de noter que les PC standards peuvent exécuter divers types d'applications, tandis que les systèmes embarqués exécutent une seule application dédiée.
- L'interface homme-machine peut varier, allant d'une simple LED clignotante à un cockpit complexe d'avion de ligne.
- Pour améliorer les performances et la fiabilité du système embarqué, des circuits numériques ou analogiques peuvent être utilisés en complément.
- Les principaux secteurs où les systèmes embarqués sont utilisés comprennent :
- Jeux et calculs généraux : applications similaires aux applications de bureau, mais intégrées dans des systèmes embarqués, tels que les jeux vidéo, les décodeurs TV, etc.
- Contrôle de systèmes : automobiles, processus chimiques, processus nucléaires, systèmes de navigation, etc.
- Traitement du signal : radars, sonars, compression vidéo, etc.
- Communication et réseaux : transmission et commutation d'informations, téléphonie, Internet,…. [3]

4 L'architecteur d'un système embarqué :

Le schéma suivant illustre l'architecture d'un système embarqué :

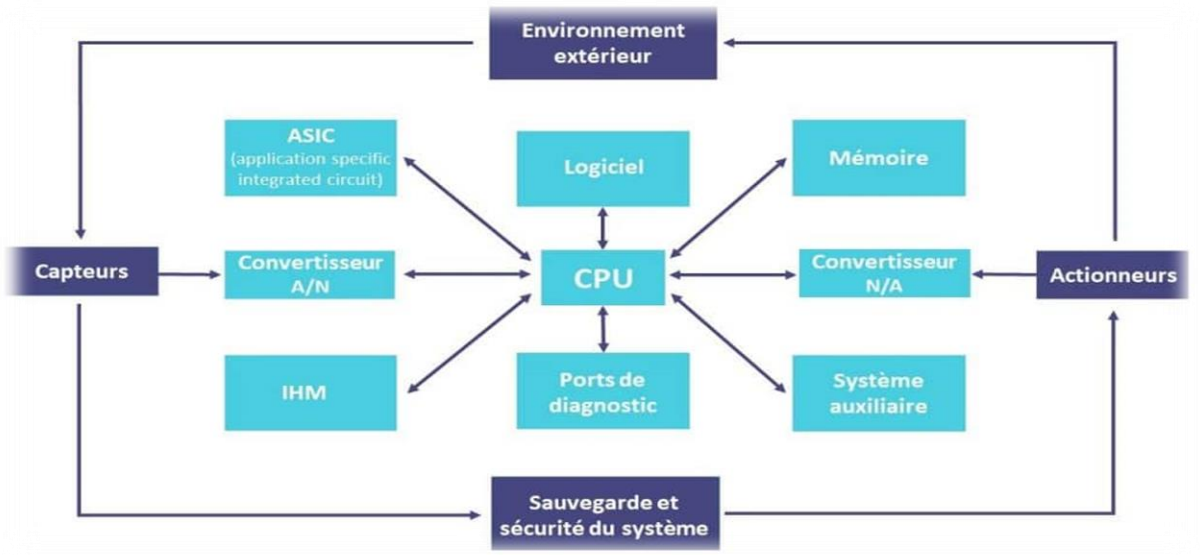


Figure 1- 2: Architecture générale d'un système embarqué

L'architecture d'un système embarqué peut varier en fonction de ses différentes catégories. Par exemple, certains systèmes autonomes ne nécessitent pas de composants auxiliaires. Néanmoins, une architecture de base comprend généralement plusieurs éléments essentiels. On y trouve une unité centrale de traitement (CPU), un système d'exploitation qui peut parfois être un logiciel spécifique, ainsi que divers capteurs tels que des capteurs de température, des capteurs de vibrations, des accéléromètres, des GPS, etc. En outre, des actionneurs tels que des moteurs, des vérins et même des buzzers font partie intégrante de cette architecture. Bien que facultative, une interface utilisateur (IHM) peut être utilisée pour reconfigurer le système ou vérifier son bon fonctionnement.

Le fonctionnement du système peut être résumé de la manière suivante :

- Les informations provenant de l'environnement extérieur sont détectées par différents capteurs.
- Les données capturées par les capteurs sont converties en format numérique pour un traitement en temps réel. Ce traitement est effectué à l'aide de composants logiciels embarqués, comprenant le CPU, l'ASIC et tout autre système auxiliaire.
- Les résultats de ce traitement génèrent des commandes, qui sont ensuite transmises aux actionneurs, tels que des moteurs, afin de modifier l'environnement extérieur. [4]

5 Les compositions d'un système embarqué :

Quel que soit le type ou la complexité du système, un système embarqué (voir Figure 1) se compose de deux parties principales :

- Une partie matérielle, qui est responsable des performances du système.
    - Cela inclut des composants tels que des microprocesseurs, des microcontrôleurs, et des DSP (Digital Signal Processors) pour le traitement des signaux.
    - Des mémoires sont également présentes pour le stockage de données temporaires ou permanentes.
    - Une interface d'entrées/sorties permet la communication avec d'autres dispositifs externes.
- Une partie logicielle, qui assure le fonctionnement du système.
    - Cette partie est constituée de programmes qui sont exécutés par le matériel embarqué.
    - Les programmes sont développés pour réaliser des tâches spécifiques et contrôler le système. [5]

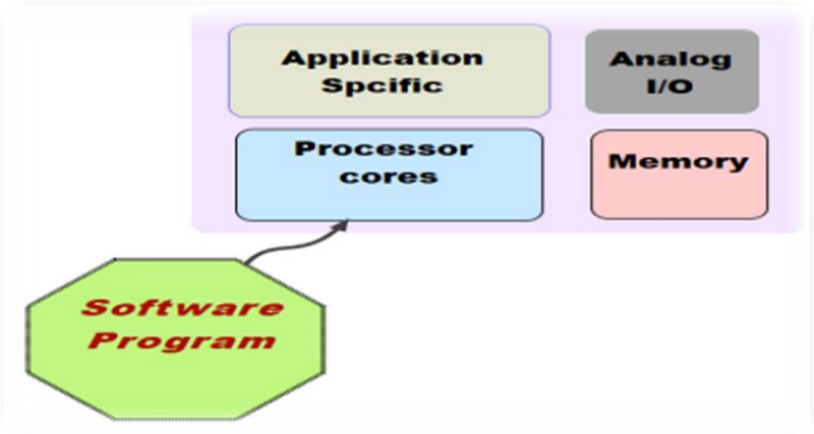


Figure 1- 3 : Composition d'un système embarquée

La composition d'un système embarqué inclut généralement les éléments suivants :

1) **Le processeur :** Il est le cerveau du système et est responsable de l'exécution des instructions. Le processeur peut être un processeur généraliste comme un processeur Intel ou un processeur spécialisé comme un processeur ARM.

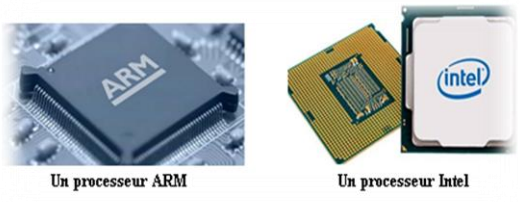


Figure 1- 4 : Processeur

2) **La mémoire :** La mémoire est utilisée pour stocker les programmes, les données et les résultats intermédiaires. Les types de mémoire utilisés peuvent inclure la RAM, la ROM, la Flash ou l'EEPROM.

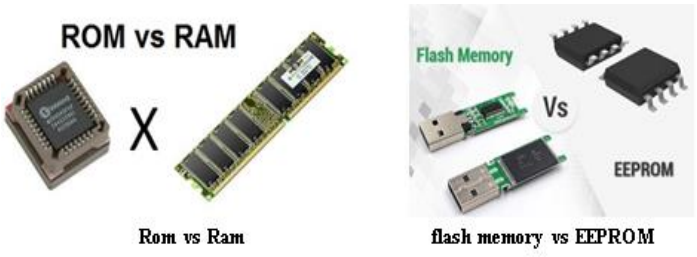


Figure 1- 5 : La Mémoire

3) **Le périphérique d'entrée-sortie (E/S)** : Les périphériques d'E/S sont utilisés pour interagir avec le système, par exemple pour saisir des données ou afficher des résultats. Les périphériques d'E/S courants comprennent les claviers, les écrans, les capteurs, les boutons, les DEL, etc.

Figure 1- 6: Le périphérique d'entrée-sortie(E/S)

4) **Les interfaces :** Les interfaces sont utilisées pour connecter le système à d'autres équipements et systèmes. Les interfaces communes incluent les ports série, USB, Ethernet, WIFI et Bluetooth.

Figure 1- 7 : Les interfaces

5) **Le logiciel embarqué :** le logiciel embarqué est le programme qui contrôle le fonctionnement du système. Il peut être écrit en langage de programmation de bas niveau ou haut niveau tels que C/C++, Python, Java, etc.

Figure 1- 8: Les logiciels embarqués

6) **Les alimentations :** Les systèmes embarqués peuvent être alimentés par une batterie, un adaptateur secteur ou une source d'énergie renouvelable.

Figure 1- 9: Les alimentations

6 L'art de bien concevoir un système embarqué :

Les caractéristiques essentielles d'un système embarqué comprennent :

- Robustesse : garantir la résistance du système face à des conditions difficiles.
- Simplicité : privilégier une conception et une maintenance simplifiées.
- Fiabilité : assurer un fonctionnement correct et constant du système.
- Fonctionnalité : répondre aux besoins spécifiques pour lesquels il a été conçu.
- Sécurité : accorder une importance particulière à la sécurité des personnes.
- Tolérance aux erreurs : permettre au système de gérer les erreurs et les problèmes éventuels.

Parallèlement, d'autres contraintes doivent être prises en compte :

- Encombrement : s'adapter à des espaces restreints.
- Poids : tenir compte des considérations de poids, notamment pour les applications portables.
- Packaging : relever le défi de l'intégration de l'électronique analogique, numérique et des composants RF dans un espace limité sans interférences.
- Environnement externe : considérer les conditions dans lesquelles le système embarqué fonctionnera.
- Consommation électrique : minimiser la consommation électrique, en particulier pour les systèmes portables alimentés par batterie, afin de réduire les coûts liés à l'utilisation de batteries de plus grande capacité.
- Coût : assurer des coûts de production extrêmement bas pour les systèmes embarqués fabriqués en grande série.
- Temps de développement : être en mesure de développer un système opérationnel rapidement pour rester compétitif sur le marché.

Face à ces contraintes, les concepteurs suivent des principes de bon sens, notamment :

- Simplicité : privilégier des solutions simples plutôt que complexes.
- Utilisation de solutions existantes ou développées par d'autres pour gagner en efficacité.
- Évaluation de la pérennité à long terme avant d'adopter des technologies de pointe.
- Prudence dans l'adoption des derniers composants disponibles, en particulier pour les applications nécessitant une maintenance sur une longue période, comme dans le domaine de la défense.
- Utilisation de technologies éprouvées et fiables, même si elles peuvent avoir un certain retard par rapport aux avancées grand public. [3]

7 Domaine d'application des systèmes :

Les systèmes embarqués sont désormais largement utilisés dans diverses applications. Ils se retrouvent dans le domaine du transport, notamment dans l'avionique, l'aérospatiale, l'automobile et le secteur ferroviaire. De plus, les systèmes embarqués sont présents dans de nombreux appareils électriques et électroniques tels que les appareils photo, les jouets, les postes de télévision, les appareils électroménagers, les systèmes audio et les téléphones portables. Ils sont également utilisés dans des domaines tels que la distribution d'énergie et l'automatisation. (Figure 3) [5]

Figure 1- 10 : Domaines d'application des systèmes embarqués

8 Problèmes de sécurité dans les systèmes embarqués :

8.1 Concepts de base de la sécurité :

La sécurité des systèmes embarqués englobe diverses préoccupations spécifiques, telles que la préservation de la confidentialité, de l'intégrité et de la disponibilité des données.

8.1.1 La confidentialité :

La confidentialité vise à empêcher les utilisateurs non autorisés d'accéder aux informations sensibles stockées ou transmises par le système embarqué, telles que les données personnelles, les codes sources, les schémas de conception, etc. Seules les personnes autorisées peuvent y accéder. Une grande partie de la recherche en sécurité informatique se concentre sur la protection de la confidentialité.

Pour assurer la confidentialité, différentes techniques peuvent être mises en œuvre, notamment :

- Le contrôle d'accès au système embarqué (SE), qui régule l'accès aux fonctionnalités du système.
- Le contrôle d'accès aux ressources internes du SE, qui gère l'accès aux différentes ressources internes du système embarqué.

8.1.2 L'intégrité :

L'intégrité des données assure que les données présentes dans le système embarqué n'ont pas été supprimées ou modifiées sans autorisation, que ce soit suite à une erreur, à une action malveillante de l'utilisateur ou à l'infection par un virus.

8.1.3 La disponibilité :

La disponibilité se réfère à la capacité d'accéder au système embarqué lorsqu'il est nécessaire, sans retard injustifié, par une entité autorisée. Par exemple, la disponibilité implique la prévention des attaques de déni de service. Il est important de noter que l'accessibilité d'un système ne garantit pas automatiquement sa disponibilité, car le système doit également fonctionner correctement et remplir sa fonction de manière adéquate. [6]

9 Les attaques dans les systèmes embarqués :

9.1 Sources d'attaques dans les systèmes embarqués :

Les systèmes embarqués sont exposés à plusieurs types d'attaques, dont la principale cause réside dans les faiblesses et les erreurs lors de la mise en œuvre des mécanismes de sécurité fonctionnelle et des algorithmes de cryptographie. Ces faiblesses permettent aux attaquants de contourner ou d'affaiblir considérablement la solution de sécurité. Les raisons sont les suivantes :

9.2 Utilisation de clés de cryptographie faibles :

Les systèmes embarqués utilisent souvent des algorithmes de cryptographie pour protéger les données sensibles. Cependant, si des clés de cryptographie faibles sont utilisées, elles peuvent être facilement compromises par des attaquants. Par exemple, l'utilisation de clés courtes ou prédictibles rend le système vulnérable à des attaques par force brute ou par analyse statistique.

9.3 Réutilisation de codes et de composants non sécurisés :

Les développeurs de systèmes embarqués peuvent réutiliser des codes et des composants provenant de sources tierces sans tenir compte de leur sécurité. Cela peut introduire des vulnérabilités dans le système, car les codes et les composants peuvent contenir des failles de sécurité connues ou des portes dérobées.

A. Manque de tests de sécurité approfondis :

Les tests de sécurité sont essentiels pour identifier les vulnérabilités et les faiblesses d'un système embarqué. Cependant, en raison de contraintes de temps ou de ressources, les tests de sécurité peuvent être insuffisants, ce qui permet aux attaquants de trouver des failles non détectées. [7]

10 Types d'attaque :

Les menaces qui peuvent effectuer les systèmes embarqué incluent plusieurs types attaquants, voici quelques exemples :

- ✓ **Les hackers :** ce sont des personnes qui cherchent à exploiter les failles de sécurité pour accéder à des informations ou à des systèmes auxquels ils ne devraient pas avoir accès.

- ✓ **Les pirates informatiques :** ce sont des individus qui cherchent à pénétrer un système informatique pour y voler des données ou y installer des logiciels malveillants.
- ✓ **Les crackers *:*** ces personnes ont pour objectif de casser des mots de passe ou des codes d'accès pour accéder à des données protégées.
- ✓ **Les employés malveillants *:*** ces personnes sont des employés d'une entreprise qui cherchent à utiliser leur accès privilégié à des données pour les voler ou les détruire.
- ✓ **Les groupes de hackers organisés *:*** ce sont des groupes de personnes qui se coordonnent pour mener des attaques ciblées sur des entreprises, des gouvernements ou des institutions.
- ✓ **Les cybers terroristes :** ces individus cherchent à causer des dommages importants à des infrastructures critiques telles que les réseaux électriques ou les systèmes de transport en commun. [8]

11 Classification des attaques :

Il est possible de classifier les attaques en se basant sur 2 critères : L'objectif fonctionnel et les méthodes utilisées afin d'exécuter ces attaques.

11.1 Critère 1 : L'objectif fonctionnel :

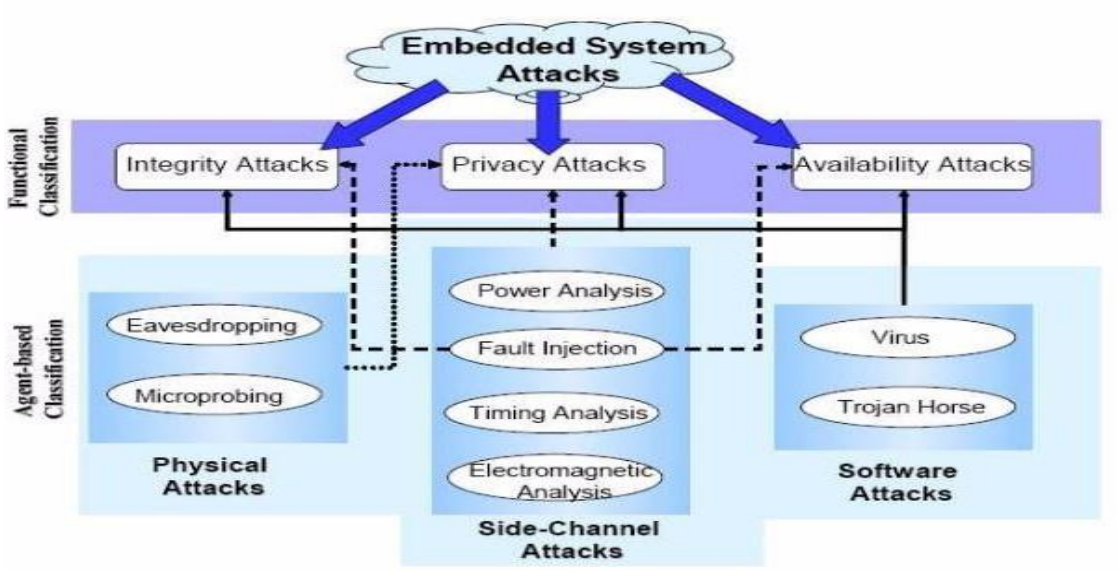


Figure 1- 11 : Classification des attaques dans les systèmes embarqués

La classification générale des attaques sur les systèmes embarqués est présentée dans la Figure 2. [9]Au premier niveau de cette classification, l'objectif fonctionnel des attaques est pris en compte, ce qui permet de distinguer trois types d'attaques :

- ✓ **Attaques de confidentialité :** Elles ont pour but de récupérer des informations sensibles stockées, transmises ou manipulées par un système embarqué.
- ✓ **Attaque d'intégrité :** Leur objectif est de modifier les données ou le code associés à un système embarqué.
- ✓ **Attaque sur la disponibilité :** Ces attaques visent à introduire des erreurs afin de perturber le fonctionnement normal d'un système ou de s'approprier les ressources, entraînant ainsi une indisponibilité du système pour son fonctionnement habituel.

11.2 Critère 2 : les méthodes utilisées :

Dans la Figure 2, le deuxième niveau et la Figure 3 présentent une classification des attaques basée sur les méthodes et les agents utilisés pour les déclencher. Ces agents sont généralement regroupés en trois catégories principales :

- ✓ **Attaques physiques :** Ce type d'attaques requiert une intrusion physique dans le système embarqué et implique une manipulation directe du matériel
- ✓ **Attaque des logiques :** Ces attaques sont lancées par des agents logiciels tels que les virus, les chevaux de Troie et d'autres formes de programmes malveillants..
- ✓ **Les canaux cachés :** Ce type d'attaques repose sur l'observation des caractéristiques du système lors de l'exécution d'opérations de chiffrement. Cela peut inclure des mesures telles que la consommation d'énergie, le temps d'exécution ou le comportement face à des vulnérabilités.

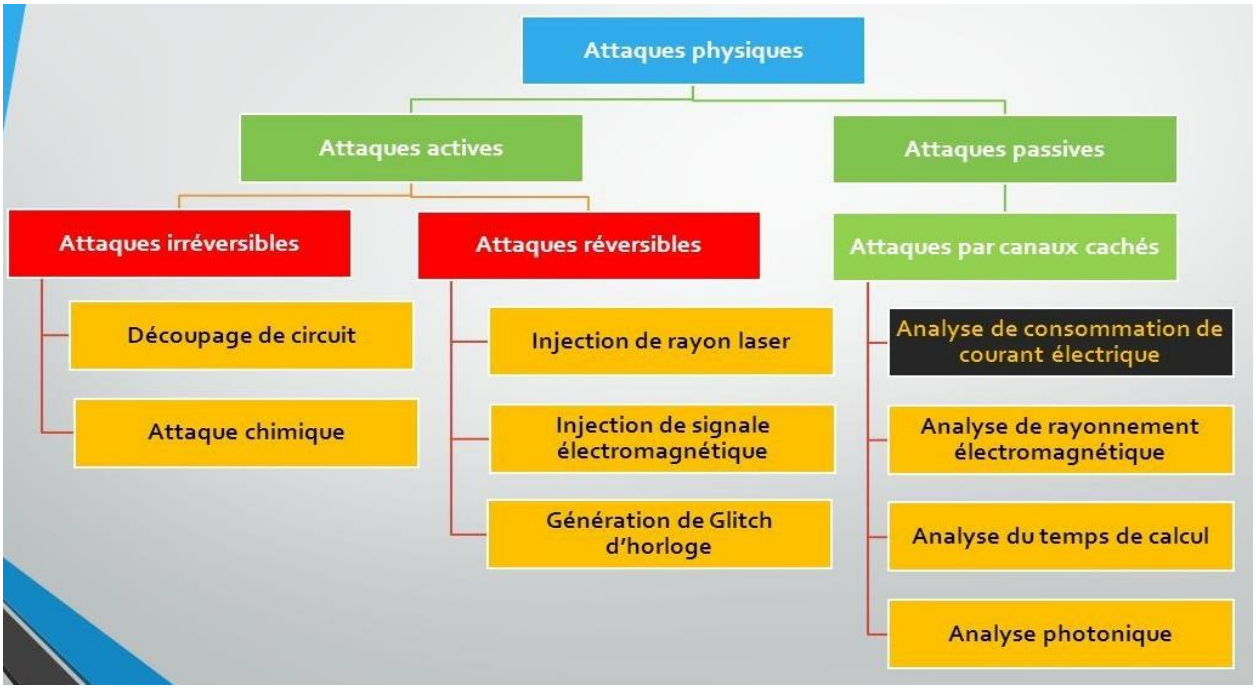


Figure 1- 12 : Classification des attaques dans les systèmes embarqués selon les méthodes utilisée **[10]**.

12 Conclusion :

En conclusion, les systèmes embarqués jouent un rôle essentiel dans de nombreux domaines, de l'automobile aux dispositifs médicaux en passant par les objets connectés. Cependant, ces systèmes présentent des problèmes de sécurité significatifs. Leur nature complexe, associée à des ressources limitées et des contraintes de temps réel, crée des vulnérabilités potentielles. Les cyberattaques visant les systèmes embarqués peuvent compromettre la confidentialité, l'intégrité et la disponibilité des données, avec des conséquences graves pour la sécurité des individus et des infrastructures. Des mesures de sécurité robustes, telles que la conception sécurisée, la gestion des accès et les mises à jour régulières, sont indispensables pour atténuer ces risques. Une collaboration entre les fabricants, les développeurs, les chercheurs en sécurité et les régulateurs est nécessaire pour faire face à ces défis et garantir la protection des systèmes embarqués dans un monde de plus en plus interconnecté.

Chapitre 2 :
Carte à Puce

Chapitre 2 : Carte à Puce

1 Introduction :

Une carte à puce est un dispositif électronique embarqué dans une petite carte en plastique. Elle est dotée d'une puce électronique intégrée qui contient un microprocesseur et de la mémoire. Les cartes à puce sont utilisées dans les systèmes embarqués pour stocker, traiter et sécuriser des informations sensibles de manière fiable.

Ces cartes offrent un large éventail d'applications dans différents domaines, tels que les transactions financières, l'identification personnelle, le contrôle d'accès, la gestion des identités, le stockage sécurisé des données, et bien plus encore. La présence d'une puce électronique permet à la carte d'exécuter des programmes et des algorithmes spécifiques, ce qui lui confère des capacités de traitement avancées.

Les cartes à puce sont particulièrement appréciées pour leur sécurité renforcée. Les informations stockées sur la carte sont protégées par des mesures de sécurité telles que le chiffrement et les codes d'accès. Cela garantit la confidentialité et l'intégrité des données, ce qui est essentiel dans les applications qui impliquent des informations sensibles.

Grâce à leur format compact, les cartes à puce sont faciles à transporter et à intégrer dans divers appareils et systèmes. Elles sont utilisées dans de nombreux secteurs, tels que les services bancaires, les télécommunications, les transports, la santé, l'administration publique, les cartes d'identité, les passeports et bien d'autres.

En résumé, les cartes à puce sont des dispositifs embarqués dans une petite carte en plastique, contenant une puce électronique. Elles sont largement utilisées dans les systèmes embarqués pour stocker, traiter et sécuriser des informations sensibles dans une variété de domaines. Leur sécurité renforcée, leur polyvalence et leur format compact en font un choix privilégié pour de nombreuses applications.

1.1 Présentation de la carte à puce

Une carte à puce est un objet en plastique contenant un circuit micro-électronique qui possède des fonctionnalités similaires à celles d'un micro-ordinateur. Sa portabilité, permettant de la ranger dans un portefeuille, ainsi que sa capacité à sécuriser les données et les programmes contre les attaques, jouent un rôle essentiel dans le stockage de clés et l'exécution d'algorithmes cryptographiques pour les applications mobiles nécessitant un niveau élevé de sécurité [11]. Ces utilisations incluent notamment :

- ✓ La sécurisation des transactions (cartes bancaires).

✓

✓ L'identification et le contrôle d'accès (passeport électronique).

La Figure 2.1 illustre les contacts d'un module de carte à puce, composé de 8 zones :

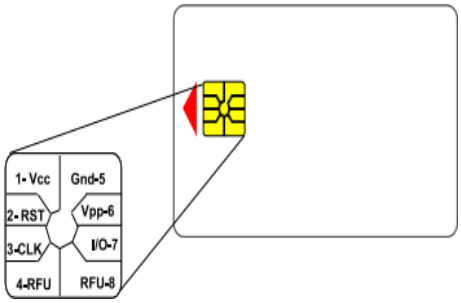


Figure 2- 1: Les contacts d'un module de carte à puce

Elle est divisée en 8 zones distinctes [11] :

1. Vcc : Il s'agit de la zone qui fournit la tension d'alimentation à la carte.
2. RST : Cette zone est dédiée au signal de remise à zéro de la carte.
3. CLK : Il s'agit de l'horloge fournie par le lecteur à la carte.
4. RFU : Cette zone est réservée pour une utilisation future.
5. Gnd : potentiel de référence (masse).
6. Vpp : Auparavant, cette zone était utilisée pour la tension de programmation (21 volts) permettant d'alimenter une pompe de charge lors des écritures en EEPROM, mais elle n'est plus utilisée de nos jours.
7. I/O : Cette zone est une ligne bidirectionnelle permettant le transfert des données entre la carte et le lecteur.

1.2 Composants essentiels d'une carte à puce :

La structure physique d'une carte à puce se compose de trois éléments distincts :

- ✓ La carte plastique : C'est le support physique de base de la carte à puce. Il s'agit d'une carte en plastique qui abrite les composants électroniques.
- ✓ Le micromodule : Ce module électronique est intégré à l'intérieur de la carte plastique. Il renferme la puce et les autres éléments nécessaires au fonctionnement de la carte.
- ✓ La puce : La puce électronique se trouve à l'intérieur du micromodule. Elle contient les données et le programme nécessaires à l'exécution des tâches de la carte à puce. La puce est reliée aux contacts présents sur le micromodule, qui servent d'interface pour la

communication avec le lecteur externe. Ces contacts sont la seule partie visible depuis l'extérieur de la carte. [12]

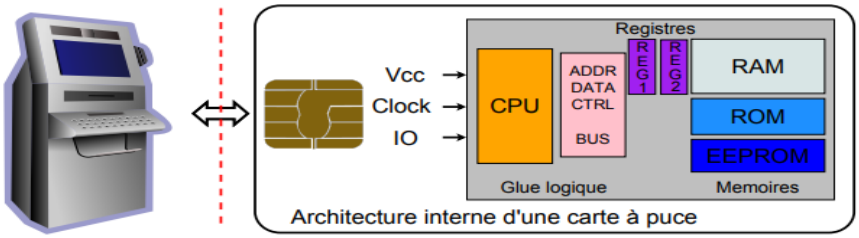


Figure 2- 2: Schéma simplifié d'une carte à puce

2 Familles et types de cartes :

2.1 Familles de carte à puce :

Différentes catégories de cartes à puce existent, offrant des fonctionnalités spécifiques :

- Les cartes à mémoire simple : Ces cartes servent essentiellement de support de stockage. Elles permettent de stocker et de récupérer des données, mais ne sont pas capables d'exécuter des opérations logiques avancées.
- Les cartes à mémoire avec logique câblée : Ces cartes disposent d'un support de stockage et sont capables d'effectuer des opérations de logique simple. Elles peuvent effectuer des tâches telles que la comparaison de données ou la réalisation de calculs de base.
- Les cartes à microprocesseur : Également appelées cartes "intelligentes", ces cartes possèdent une mémoire programmable et offrent des fonctionnalités avancées pour effectuer des opérations logiques complexes. Elles peuvent être programmées pour prendre des décisions en fonction des instructions reçues. Cela leur confère une certaine forme d'intelligence, d'où leur appellation**.** [12]

2.2 Types de cartes :

En matière de communication avec le lecteur, il existe deux principaux types de cartes à puce qui se distinguent :

- Les cartes sans contact : Ces cartes utilisent la technologie RFID (Identification par Radio Fréquence) et permettent une communication sans contact physique avec le lecteur. Elles utilisent des ondes radio pour échanger des données, sans nécessiter un contact direct avec le lecteur. Cependant, l'alimentation en courant de la carte est généralement fournie par le terminal ou le lecteur auquel elle est connectée.
- Les cartes à contact : Ces cartes requièrent un contact physique direct avec le lecteur au niveau du micromodule de la carte. Ce contact physique permet de transmettre l'alimentation électrique

et les commandes entre la carte et le lecteur. Les données sont échangées via cette connexion directe entre les contacts de la carte et les broches du lecteur. [12]

3 Présentation de la technologie RFID :

La technologie de radio-identification (RFID) est une méthode d'identification automatique similaire à la reconnaissance optique de caractères ou aux codes-barres. Contrairement aux codes-barres, qui nécessitent une lecture optique, la RFID utilise des ondes électromagnétiques pour transférer des informations, ce qui permet de lire plusieurs étiquettes simultanément.

La particularité de la RFID réside dans sa capacité à fonctionner à distance selon le principe suivant : un lecteur émet un signal radio et reçoit les réponses des étiquettes ou des tags présents dans sa zone d'action. Les systèmes RFID sont variés, offrant différents types de mémoire, fréquences, portées et modes d'alimentation. Grâce à cette technologie, il est possible de lire les étiquettes même sans avoir une ligne de vue directe, et elle peut même traverser des matériaux minces. [13]

3.1 Que sont les cartes RFID ?

Les cartes sans contact intègrent une puce RFID (Identification par Radio Fréquence) qui stocke toutes les informations requises. Les données sont transmises via des ondes radio et captées par un lecteur RFID. Une fois captées, ces données sont décodées par le lecteur puis transmises à un logiciel intégré pour analyse et présentation. Ce processus global est à la fois rapide et fiable, s'effectuant en quelques secondes seulement.

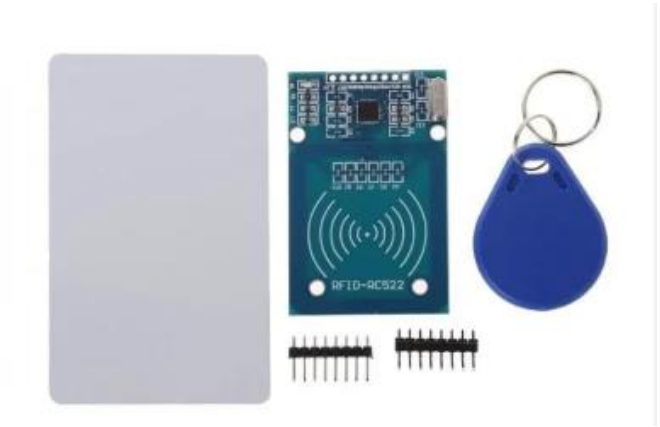


Figure 2- 3: Carte à puce RIFD

Contrairement aux cartes magnétiques ou aux codes-barres traditionnels, l'utilisation des cartes RFID ne nécessite pas de les glisser pour lire les informations encodées. Au lieu de cela, les cartes RFID requièrent simplement d'être à proximité du lecteur, qui capte les signaux et effectue rapidement la transaction. [13]

3.2 Les catégories de puces RFID :

Il y a trois types de puces RFID différents :

- ✓ Les puces passives.
- ✓ Les puces actives.

- ✓ Les puces intelligentes.

- Les puces passives fonctionnent sans batterie. Elles sont activées par un système qui transmet des ondes magnétiques.
- Les puces actives, quant à elles, sont équipées d'une batterie. Elles n'ont pas besoin d'être activées et transmettent les informations de manière autonome à un récepteur.
- Enfin, les puces intelligentes sont dotées d'un système de sécurité permettant de crypter les informations stockées. Pour accéder aux données, une identification est nécessaire. Un exemple concret serait celui des cartes bancaires. [13]

4 Les familles de puces RFID

Il existe différentes familles parmi les trois catégories de puces suivantes :

- ✓ Les puces d'étiquettes en lecture seule :

Dans cette première catégorie, les puces sont non modifiables. Lors de leur fabrication, le fabricant enregistre les identifiants et les données dans la puce. Un avantage de ces puces est qu'elles sont moins coûteuses que les autres.

- ✓ Les puces d'étiquettes à écriture seule et lecture multiple :

Dans la deuxième catégorie, les puces sont également non modifiables en termes de contenu. Cependant, elles peuvent être lues plusieurs fois sur différents lecteurs.

- ✓ Les puces d'étiquettes à écriture et lecture multiples :

La troisième catégorie regroupe les puces offrant un contenu pouvant être modifié plusieurs fois. Elles peuvent également être lues plusieurs fois sur différents lecteurs. Les cartes de transport et les systèmes de contrôle d'accès aux immeubles sont des exemples d'utilisations de ces puces. [13]

5 Constitutifs d'un système RFID :

Un système RFID, tel qu'illustré dans la Figure-1, est composé de plusieurs éléments de base :

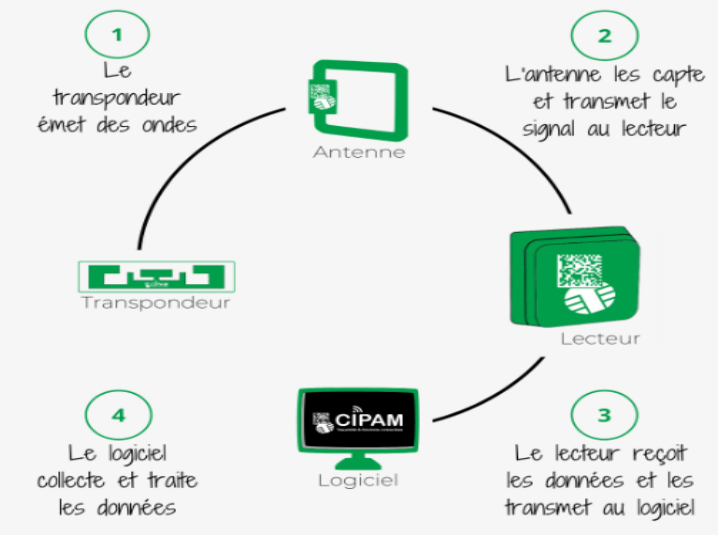


Figure 2- 4 : Constitutifs d'un système RFID

Une étiquette (parfois appelée transpondeur ou Tag) qui se compose d'une puce à semi-conducteur, d'une antenne et, dans le cas où le système est actif, d'une batterie. Elle est attachée à un objet et comprend une antenne et une puce de données pour la sauvegarde d'informations telles que son identifiant.

- Un lecteur (parfois appelé interrogateur ou dispositif de lecture/écriture) qui comprend une antenne, un module électronique RF (Radio Fréquence) et un module de contrôle.
- Un contrôleur (parfois appelé host) qui prend généralement la forme d'un PC ou d'une base de données, d'un poste de travail et d'un logiciel de commande. Ce système de gestion de données stocke les informations fournies par le lecteur lors de l'interrogation de l'étiquette. [14]

6 Comment fonctionnent les cartes d'accès RFID :

Comme expliqué précédemment, les cartes RFID renferment une puce RFID contenant des informations spécifiques pour chaque individu. Ces informations peuvent être transmises à un lecteur RFID via des ondes radio.

Lorsque le titulaire de la carte s'approche d'un lecteur, la puce est activée par les ondes électromagnétiques émises par ce dernier. Elle émet ensuite des signaux radio qui sont captés par le lecteur. Ainsi, le lecteur récupère et interprète les données du titulaire de la carte.

Deux principaux types de cartes d'accès RFID sont présents sur le marché :

- ✓ Les cartes de proximité RFID : Ces cartes simples permettent une transmission unidirectionnelle des données de la carte vers le scanner/lecteur. Elles nécessitent simplement d'être à proximité du lecteur pour transmettre les informations.

- ✓ Les cartes à puce RFID : Ces cartes offrent un niveau de contrôle d'accès plus sécurisé et rapide que les cartes de proximité. Elles possèdent une fonctionnalité unique qui leur permet de communiquer avec les lecteurs de cartes RFID, ce qui permet d'utiliser un cryptage avancé. De plus, ces cartes sont équipées de processeurs intégrés qui contribuent à l'authentification de l'utilisateur grâce à un code crypté à usage unique. Ce code expire immédiatement après utilisation, rendant ainsi la duplication de la carte difficile pour les criminels. [13]

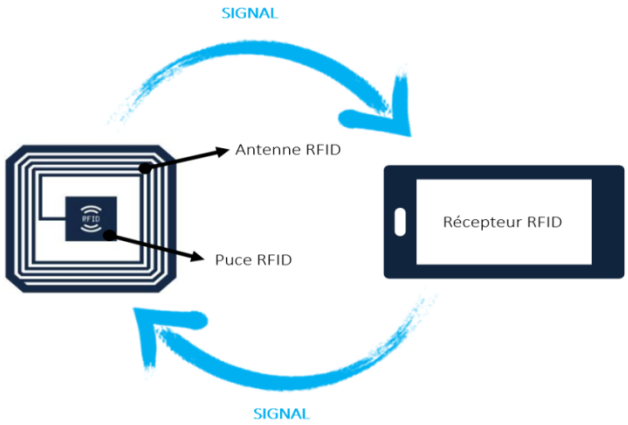


Figure 2- 5 : Fonctionnent les cartes d'accès RFID

7 Comment le système communique ?

Le Tag et le lecteur établissent une communication à l'aide d'ondes radio. Lorsqu'un objet étiqueté pénètre dans la zone de couverture d'un lecteur, ce dernier envoie un signal demandant à l'étiquette de transmettre les données qu'elle contient Les étiquettes sont capables de stocker diverses informations concernant les objets auxquels elles sont attachées, telles que des numéros de série, la taille de l'objet et d'autres données pertinentes. Une fois que le lecteur a reçu ces données, il les transmet au contrôleur par le biais d'une interface réseau standard, telle qu'un LAN Ethernet. Le contrôleur peut ensuite utiliser ces informations à des fins diverses.

Par exemple :

Le contrôleur peut utiliser les données pour créer une sauvegarde simple des objets dans une base de données, ou pour effectuer un traitement plus avancé des informations.

Un système RFID peut être constitué de plusieurs lecteurs disséminés sur une vaste surface, telle qu'un entrepôt. Cependant, tous ces lecteurs peuvent être gérés en réseau par un seul contrôleur. De même, un lecteur simple peut communiquer simultanément avec plusieurs étiquettes. En réalité, grâce aux progrès technologiques actuels, il est possible de réaliser une communication simultanée avec un taux pouvant atteindre 1000 étiquettes par seconde, avec une précision dépassant les 98%. [15]

8 Classification des cartes RFID basée sur la longueur d'onde de fréquence de la puce RFID

Les cartes RFID peuvent être classées selon le type de puce RFID utilisée lors de leur fabrication. On distingue principalement trois catégories de cartes RFID :

8.1 Cartes RFID basse fréquence (LF)

Ces cartes sont équipées de tags RFID LF (30 kHz à 300 kHz). Elles ont une vitesse de lecture plus lente et une portée relativement courte.

Toutefois, ces cartes conservent leur fonctionnalité même en présence de métaux et de liquides, ce qui les rend utilisables dans des environnements humides et métalliques.

8.2 Cartes RFID haute fréquence

Ces cartes fonctionnent dans une plage de fréquences allant de 3 MHz à 30 MHz. Elles offrent une meilleure capacité de stockage et une portée de lecture plus étendue que les cartes basse fréquence. Elles sont donc particulièrement adaptées à des applications telles que la gestion de bibliothèques et de transports.

8.3 Cartes RFID à ultra-haute fréquence (UHF) :

Ces cartes opèrent dans une plage de fréquences allant de 300 MHz à 3 GHz. Elles sont moins coûteuses que les cartes LF et haute fréquence. Elles sont couramment utilisées pour le suivi des actifs et la gestion des stocks. [16]

9 Description détaillée des composants des cartes RFID

Lorsque vous examinez une carte RFID classique, il y a peu de différence apparente par rapport à une carte en plastique ordinaire. Cependant, sa véritable singularité ne se révèle que lors de son utilisation pour effectuer des paiements à l'épicerie ou pour ouvrir la porte de votre bureau.

Mais qu'est-ce qui rendent les cartes RFID si particulières ? Pourquoi semblent-elles posséder une capacité quasi magique qui leur permet de communiquer sans nécessiter de connexion physique ? Voici les éléments constitutifs qui leur permettent de fonctionner.

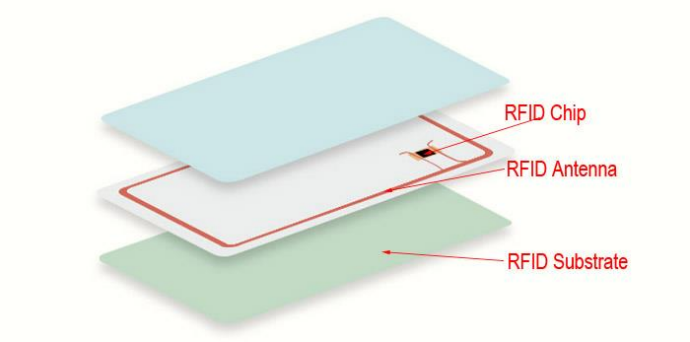


Figure 2- 6 : Composant cartes RFID

A. Puce RFID

La puce RFID constitue la principale différence entre les cartes RFID et les cartes en plastique ordinaires. Elle est composée d'une minuscule puce informatique intégrée à la carte, contenant des informations relatives à votre identité et aux détails de votre compte. Malgré sa petite taille (environ celle d'un grain de riz), cette puce sophistiquée peut stocker des milliers d'octets de données. Toutefois, elle dépend d'une alimentation électrique externe pour fonctionner, car elle ne possède pas sa propre source d'énergie.

B. Antenne

L'antenne, une petite bobine métallique intégrée à la carte, joue un rôle essentiel dans la communication de la puce avec un lecteur. Elle est capable de recevoir et d'émettre des ondes radio. Lorsqu'elle reçoit un signal radio provenant du lecteur, elle le convertit en énergie électrique. Cela permet à la puce de s'activer et de traiter les données qu'elle contient.

C. Substrat

Le substrat correspond à la partie visible et tangible de la carte. Il assure le maintien conjoint de la puce et de l'antenne, tout en fournissant une structure solide. Habituellement fabriqué en plastique, le substrat peut également être réalisé en PVC, en PET, en ABS, en bois ou d'autres matériaux robustes pour une meilleure durabilité, notamment dans le cas de cartes RFID haut de gamme. Lorsque les cartes sont exposées à des conditions physiques difficiles, il est recommandé de choisir un substrat rigide afin de garantir une longévité accrue. Par exemple, les cartes RFID époxy sont couramment utilisées dans les environnements industriels en raison de leur capacité à résister aux températures extrêmes, aux produits chimiques et à d'autres risques environnementaux. [16]

10 Présentation de la carte à puce RFID Mifare Classic 1K:

a) Badge Mifare 1K

Le badge Mifare 1K est une carte à puce sans contact largement reconnue dans le domaine de l'identification par badge. Il s'agit d'une carte en plastique intégrant une technologie de communication radiofréquence, permettant une interaction sans contact physique.

Figure 2- 7: Mifare card 1k

b) Technologie Mifare 1K

La technologie Mifare 1K a été pionnière en tant que circuit intégré utilisé massivement dans les systèmes de billetterie des transports publics. Principalement dédiée au contrôle d'accès, la carte sans contact MIFARE Classic 1K de NXP est également utilisée dans de nombreuses applications qui nécessitent l'utilisation de cartes à puce mémoire, sans les inconvénients liés à l'insertion physique du badge. Les transactions deviennent extrêmement rapides, un simple geste suffit pour présenter la carte devant le lecteur. Ces badges sont souvent utilisés dans les systèmes de contrôle d'accès physique aux bâtiments ou d'accès logique aux systèmes informatiques.

c) Caractéristiques techniques

- Mémoire EEPROM de 1 Ko (768 octets disponibles pour l'utilisateur).
- Antenne RFID intégrée.
- Fréquence de 13,56 MHz conforme à la norme ISO14443 A.
- Distance de lecture d'environ 1 cm à 7 cm.
- Numéro de série unique (4 octets).
- 16 secteurs distincts permettant la prise en charge de plusieurs applications.
- Chaque secteur comprend 4 blocs de 16 octets chacun.
- 2 x 48 bits de clés par secteur pour les hiérarchies principales.
- Les conditions d'accès peuvent être configurées librement en fonction de 2 niveaux de hiérarchie de clés.
- Nombre d'opérations d'écriture uniques : 100 000.
- Rétention des données : 10 ans. [17]

11 Les types d’attaque de la carte RFID :

On a 7 types d’attaque de la carte RFID les plus connue :

I. Reverse engineering

L'ingénierie inverse est une technique utilisée pour comprendre le fonctionnement interne des étiquettes et des lecteurs RFID en les démontant. Les pirates informatiques peuvent ainsi accéder aux données du circuit intégré et les analyser pour trouver des vulnérabilités. En utilisant des outils spécifiques et des environnements de développement intégrés (IDE), ils peuvent extraire la mémoire des tags RFID et examiner le code pour obtenir des informations sur la création du tag. Cela leur permet de trouver des failles de sécurité exploitables et d'atteindre leurs objectifs.

Dans un exemple concret, prenons un distributeur automatique de boissons qui utilise une carte RFID non sécurisée telle que la "MIFARE Classic 1k". Cette carte présente de multiples vulnérabilités et ne devrait pas être utilisée dans ce type d'application. Étant donné que le crédit de l'utilisateur est stocké sur la carte, il est possible de falsifier les données et de modifier le crédit de manière arbitraire. Ainsi, il serait possible d'obtenir une boisson pour seulement 10 centimes, par exemple.

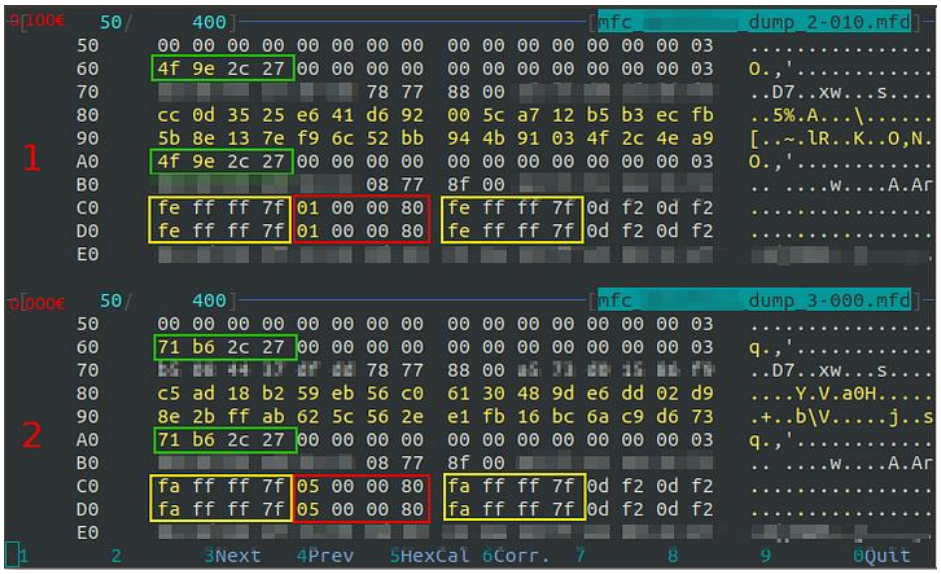


Figure 2- 8: Fichier dump d'une carte Mifare

II. Man-in-the-middle attaque or sniffing

Une attaque de l'homme du milieu se produit pendant la transmission d'un signal entre une étiquette RFID et un lecteur. Le pirate informatique écoute cette communication, l'intercepte et manipule les informations échangées. Le pirate se positionne entre l'étiquette et le lecteur, détourne le signal original et envoie de fausses données tout en se faisant passer pour un composant légitime du système RFID.

Avec l'amélioration de la portée des transmissions, cette attaque devient une menace de plus en plus sérieuse. En effet, certains lecteurs/émetteurs RFID peuvent atteindre une portée de 25 mètres, ce qui donne au pirate une plus grande étendue d'action

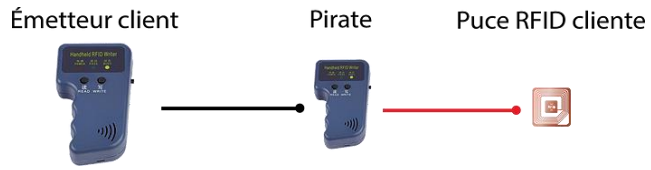


Figure 2- 9 : Mise en situation d'un man-in-the-middle

Prenons un exemple pour mieux comprendre. Supposons qu'un émetteur client souhaite communiquer avec une puce RFID cliente. Pour cela, l'émetteur doit envoyer des messages en diffusion (broadcast). Cependant, un pirate se positionne entre les deux et récupère la communication, puis la retransmet. Le pirate peut alors se faire passer pour le véritable émetteur. À partir de là, le pirate peut entretenir une conversation avec le client, lui demander et récupérer des informations personnelles. Les deux terminaux clients ont presque aucun moyen de savoir que leurs messages sont relayés, la seule différence étant une légère latence ajoutée par ce relais.

III. Denial of service

Les attaques par déni de service sont généralement des attaques physiques visant à perturber le système RFID en bloquant les signaux radio, en utilisant des interférences sonores, en retirant ou en désactivant les étiquettes RFID. L'objectif est de rendre les tags RFID inutilisables pendant un certain laps de temps, empêchant ainsi leur fonctionnement normal.

Le fonctionnement de cette attaque est relativement simple. En utilisant une antenne puissante et en réglant l'oscillateur sur la bonne fréquence d'émission des tags RFID ciblés, il est possible d'interférer avec les ondes radio utilisées par ces tags. Il convient de noter que les fréquences de fonctionnement des tags RFID sont réparties en différentes catégories telles que 125 kHz, 433 MHz, [860-930] MHz et 13,56 MHz.

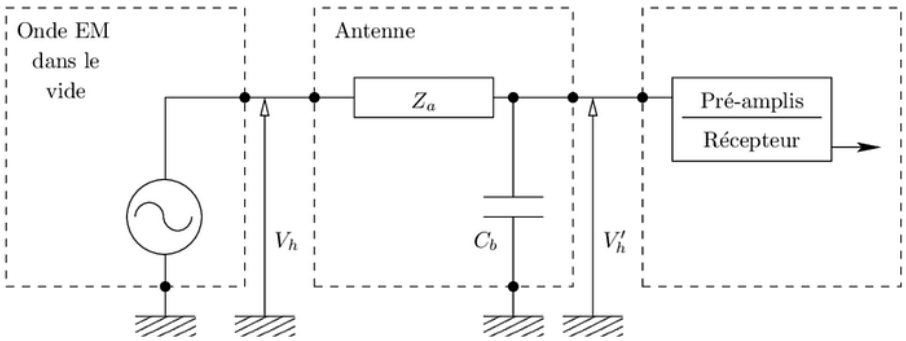


Figure 2- 10 : Schéma avec oscillateur et antenne

Prenons un exemple concret dans la vie quotidienne. Imaginez que vous vous rendez dans votre magasin de sport préféré, comme Decathlon, et que vous avez une antenne et un oscillateur électronique dans votre sac à dos. Vous pouvez paramétrer l'oscillateur pour générer des ondes à la fréquence d'émission des tags RFID du magasin, puis vous diriger vers les caisses automatiques. En émettant des ondes à pleine puissance, vous pouvez provoquer un déni de service. Les tags RFID à proximité deviendront inutilisables pendant la période pendant laquelle votre antenne émet. Il existe même des montages électroniques capables de désactiver complètement un tag RFID avec une puissance suffisante, mais cette technique est plus complexe à mettre en place que la première.

IV. Virus

Actuellement, les puces RFID n'ont pas une capacité mémoire suffisante pour stocker un virus ou un ver informatique. Cependant, à l'avenir, il est possible que les systèmes RFID deviennent vulnérables à cette menace. Un programme malveillant pourrait être injecté dans une étiquette RFID par une source inconnue, et lors de la lecture de cette étiquette dans une installation, le virus pourrait se propager au lecteur, puis au réseau et aux logiciels de l'entreprise.

Cela pourrait entraîner la paralysie des ordinateurs, des composants RFID et des réseaux connectés à ces systèmes. Cependant, il est important de noter qu'actuellement, en raison de la capacité mémoire limitée des puces RFID, une application réelle de ce type de virus n'est pas possible.

Dans un avenir proche, il est possible que les avancées technologiques permettent aux puces RFID de disposer d'une capacité mémoire plus importante, ce qui représentera un nouveau défi pour les équipes de sécurité des entreprises et les chercheurs dans ce domaine. La sécurité des systèmes RFID devra être renforcée pour prévenir de telles attaques potentielles.

V. Power analysis

L'attaque par analyse de puissance vise à surveiller les niveaux de consommation d'énergie des étiquettes RFID. Les pirates peuvent observer la différence de puissance entre un code d'accès correct et un code d'accès incorrect. En analysant les variations de consommation d'énergie, ils peuvent déduire des informations sensibles, telles que les clés de chiffrement utilisées dans le système RFID.

VI. Eavesdropping & replay

L'attaque d'écoute et de rejeu est similaire à l'attaque de l'homme du milieu, mais avec quelques différences. Elle consiste à écouter la communication entre une étiquette et un lecteur RFID, puis à enregistrer les données capturées pour les rejouer ultérieurement afin de tromper le système RFID.

Cette attaque peut être utilisée pour contourner les mécanismes de sécurité et accéder à des informations ou des ressources non autorisées.

VII. Cloning and spoofing

L'attaque de clonage et d'usurpation d'identité implique la duplication des données d'une étiquette RFID existante. Les pirates peuvent copier les informations d'une étiquette légitime et créer une étiquette clonée qui semble identique à l'originale. Ils peuvent ensuite utiliser cette étiquette clonée pour accéder à des zones sécurisées ou des objets protégés, contournant ainsi les mesures de sécurité du système RFID. [18]

12 Conclusion :

En conclusion, l'essor de la technologie RFID ouvre de nouvelles possibilités dans de nombreux secteurs, mais il soulève également des préoccupations en matière de sécurité. Les attaques potentielles sur les systèmes RFID peuvent compromettre la confidentialité des informations personnelles et financières des utilisateurs. Il est donc crucial de veiller à ce que ces technologies soient utilisées de manière responsable et sécurisée.

Il est important de prendre en compte les différentes attaques possibles, telles que l'ingénierie inverse, l'attaque de l'homme du milieu, le déni de service, le clonage et l'usurpation d'identité, ainsi que les futures menaces potentielles telles que les virus sur les puces RFID. Les entreprises et les utilisateurs doivent mettre en place des mesures de sécurité robustes pour protéger leurs systèmes RFID contre ces attaques.

Enfin, il est essentiel de suivre de près les développements et les évolutions de la technologie RFID afin de garantir une utilisation sûre et conforme, en prenant en compte les enjeux liés à la protection des données personnelles et à la sécurité des transactions.

Chapitre 3 :

Proposition d'une solution contre les attaques physiques avec une double vérification (clavier, clé mécanique)

Chapitre 3 : Proposition d'une solution contre les attaques physiques avec une double vérification (clavier, clé mécanique)

1 Introduction

Dans ce chapitre, nous nous concentrons sur la simulation de la carte Mifare Classic 1K, une étape essentielle de notre projet. Cette carte RFID est largement utilisée dans les systèmes embarqués, tels que l'accès aux salles sécurisées. Notre objectif est de reproduire virtuellement le fonctionnement de cette carte, de simuler une attaque et de proposer une solution en utilisant les bons composants matériels et logiciels.

Nous présentons également tous les composants nécessaires pour notre projet, ainsi que les étapes et astuces que nous avons suivies pour réaliser notre solution. Cette simulation s'intègre dans notre proposition globale qui consiste en une solution robuste contre les attaques physiques. Nous utilisons une double vérification via un clavier et une clé mécanique, intégrés à un système basé sur la carte RFID et Arduino Uno. Cette approche offre une sécurité renforcée tout en restant simple à mettre en œuvre.

Matériel utilisé

1.1 Unité de commande et de traitement

1.1.1 La carte Arduino UNO

Il s'agit d'une petite carte électronique mesurant 5,33 × 6,85 cm, qui est dotée d'un microcontrôleur. Ce dernier permet de programmer et de commander des actionneurs en fonction des événements détectés par des capteurs. Ainsi, la carte Arduino est une interface programmable qui offre cette fonctionnalité. **[19]**

Figure 3- 1 : La carte arduino UNO

La carte électronique ARDUINO modèle UNO est basée sur un microcontrôleur ATMEL, précisément l'ATMega328. Ce microcontrôleur ATMega328 appartient à la famille AVR et fonctionne sur une architecture 8 bits. La programmation de ce microcontrôleur peut être réalisée en utilisant le langage C. **[19]**

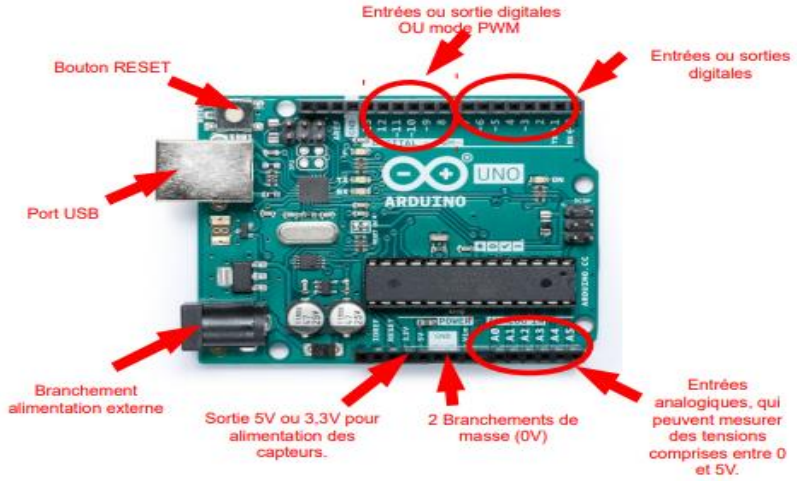


Figure 3- 2 : Les E/S d'une carte arduino UNO

1.1.2 Caractéristiques techniques de la carte Arduino UNO

- Le microcontrôleur utilisé est l'ATmega328.
- La fréquence d'horloge est de 16 MHz.
- La tension d'alimentation interne est de 5Vcc.
- La tension d'alimentation externe recommandée est de 7-12Vcc (limites : 6-20Vcc).
- Le courant maximal sur la sortie 3,3V généré par le régulateur interne est de 50mA.
- Il y a 14 broches pour les entrées/sorties binaires.
- Le courant maximal par broche en sortie est de 40 mA (85 mA en court-circuit).
- Le courant maximal cumulé par les broches en sortie est de 200 mA (soit une moyenne de 14 mA par broche).
- Les broches d'entrée/sortie binaires 0 et 1 sont utilisées pour la communication série.
- La broche S0 est utilisée pour RX et la broche S1 pour TX. Chaque broche est connectée à une LED via une résistance de 1kΩ.
- Les broches d'entrée/sortie binaires 3, 5, 6, 9, 10 et 11 sont dédiées au mode PWM.
- La broche 13 est connectée à la LED de test de la carte via une résistance de 1kΩ.
- Il y a 6 entrées analogiques, avec un niveau logique maximal de +5Vcc.
- La mémoire Flash est de 32 KB, dont 0.5 KB est utilisée par le Bootloader.
- La mémoire SRAM est de 2 KB et la mémoire EEPROM est de 1 KB.
- La carte s'interface avec un PC via un port USB.
- L'alimentation de la carte se fait par le connecteur d'alimentation (jack d'alimentation).

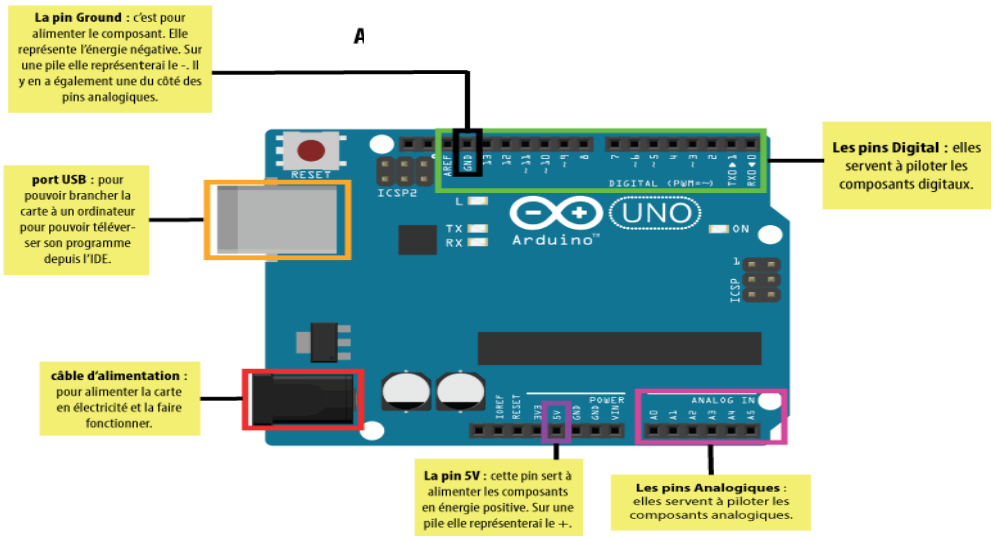


Figure 3- 3: Anatomie d'une carte Arduino UNO

2 Module RFID

a) Le module RFID RC522

Le module RFID RC522 est un dispositif permettant l'authentification sans contact à l'aide d'un badge ou d'une clé RFID. Il est conçu autour du circuit intégré Philips RC522 et utilise la fréquence de 13,56 MHz. Sa portée de communication peut atteindre jusqu'à 6 cm.

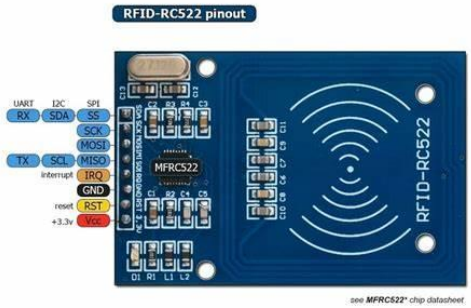


Figure 3- 4 : Module RFID RC522

- Tension : 3,3 V, courant : 13-25 mA
- Fréquence d'utilisation : 13,56 MHz, distance de fonctionnement : 0 à 60 mm. **[20]**

a) Porte clé Mifare classic 1k

Le porte-clés Mifare Classic 1K est un dispositif qui utilise une carte haute fréquence de 13,56 MHz. Cette carte possède une capacité de mémoire de 1 Ko, qui est divisée en 16 secteurs de 4 blocs chacun. Chaque bloc contient 16 octets. Ce porte-clés offre une grande flexibilité pour des applications telles que le contrôle d'accès, la billetterie des transports publics, les solutions de gestion du temps de présence, et bien d'autres. [21]

Figure 3- 5:Carte Mifare classic 1k

b) Caractéristiques

- ✓ Basée sur la puce Philips MFRC522.
- ✓ Power Voltage : 3.3V.
- ✓ Current :13-26mA.
- ✓ Fréquence d'utilisation : 13.56MHz.
- ✓ Distance opérationnelle : 0 ~ 60mm.
- ✓ Interface : SPI.
- ✓ Dimensions : 40mm × 60mm.
- ✓ Module Name : MF522-ED.
- ✓ Working current：13—26mA/ DC 3.3V.
- ✓ Standby current：10-13mA/DC 3.3V.
- ✓ Sleeping current：<80uA.
- ✓ Peak current：<30mA.
- ✓ Data communication speed：Maximum 10Mbit/s.
- ✓ Card types supported：mifare1 S50、mifare1 S70、mifare UltraLight mifare Pro mifare Desfire.
- ✓ Working temperature：-20—80 degree. [22]

1.1. Les Broches

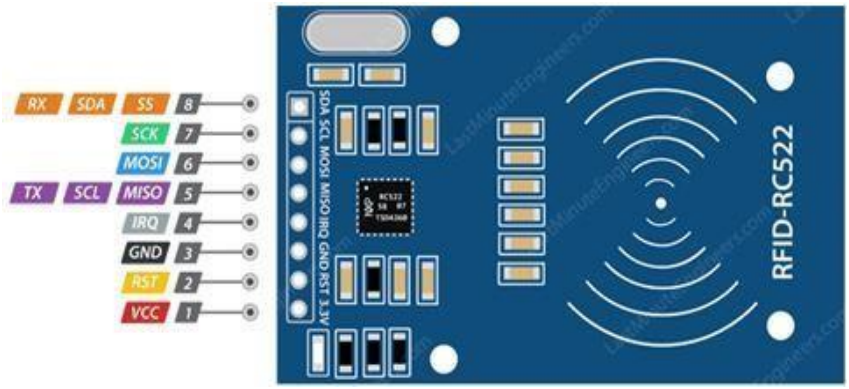


Figure 3- 6 : Module RFID MFRC522

- **L'alimentation du module, appelée Vcc** : peut être comprise entre 2,5 et 3,3 volts. Pour le connecter à votre Arduino, vous pouvez le brancher sur la sortie 3.3V. Il est important de ne pas le connecter à la broche 5V, car cela risquerait d'endommager le module.
- **La broche RST** est utilisée pour la réinitialisation et la mise hors tension. Lorsque cette broche est basse, la mise hors tension du module est activée. Cela a pour effet de désactiver tous les

composants internes, y compris l'oscillateur, et de déconnecter les broches d'entrée du monde extérieur. Lorsque la broche RST passe à l'état haut, le module est réinitialisé.

- **La broche IRQ** est une broche d'interruption qui permet d'alerter le microcontrôleur lorsque l'étiquette RFID se trouve à proximité.
- **La broche GND** est la broche de terre et doit être connectée à la broche GND de l'Arduino.
- **La broche MISO/SCL/TX** a différentes fonctions selon le mode d'interface activé. Lorsque l'interface SPI est activée, elle agit comme Master-In-Slave-Out. Lorsque l'interface I2C est activée, elle agit comme horloge série. Enfin, lorsqu'elle est en mode UART, elle agit comme sortie de données série.
- **La broche MOSI** (Master out Slave In) est l'entrée SPI du module RC522.
- **La broche SCK** (Serial Clock) accepte les impulsions d'horloge fournies par le maître du bus SPI, c'est-à-dire l'Arduino.
- **La broche SS/SDA/RX** a différentes fonctions selon le mode d'interface activé. Lorsque l'interface SPI est activée, elle agit comme une entrée de signal. Lorsque l'interface I2C est activée, elle agit comme des données série. Enfin, lorsqu'elle est en mode UART, elle agit comme une entrée de données série. Cette broche est généralement marquée par un carré pour la distinguer des autres broches. [23]

1.2. Branchement

Tableau 3.1: Brochage avec Arduino UNO. **[24]**

Pin	Wiring to Arduino Uno
SDA	Digital 10
SCK	Digital 13
MOSI	Digital 11
MISO	Digital 12
IRQ	unconnected
GND	GND
RST	Digital 9
3.3V	3.3V

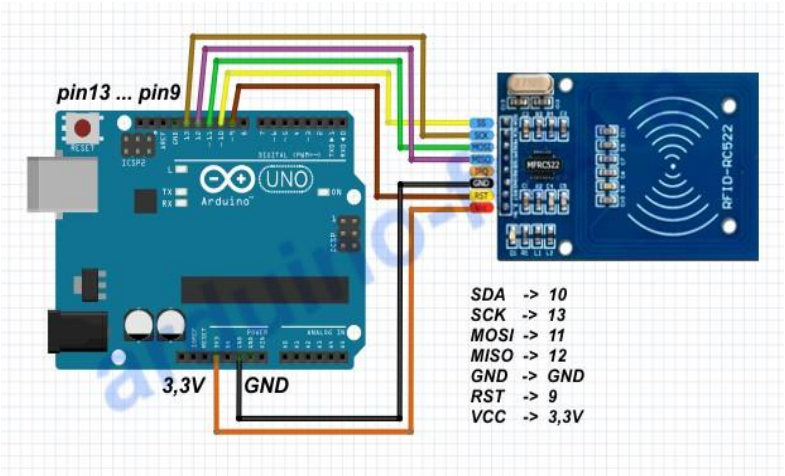


Figure 3- 7: Brochage avec Arduino UNO. **[30]**

3 L'IDE Arduino

L'IDE Arduino est un logiciel open source et gratuit, disponible en téléchargement sur le site officiel d'Arduino. Il s'agit d'un Environnement de Développement Intégré (IDE) qui offre plusieurs fonctionnalités :

- Édition de programmes : L'IDE Arduino permet d'éditer des croquis (sketches) qui sont des programmes écrits en langage C
- Compilation : Il est possible de compiler le programme dans le langage "machine" de l'Arduino. La compilation se traduit par une traduction du langage C vers le langage du microcontrôleur. La console de l'IDE fournit des informations sur le déroulement de la compilation et affiche les éventuels messages d'erreur.
- Téléversement : Le programme peut être téléversé (uploadé) dans la mémoire de l'Arduino. Ce processus de téléversement s'effectue via le port USB de l'ordinateur. Une fois le programme dans la mémoire de l'Arduino, il est appelé "micrologiciel" (firmware). La console de l'IDE fournit des informations sur le déroulement du téléversement et affiche les éventuels messages d'erreur.
- Communication : L'IDE Arduino permet de communiquer avec la carte Arduino grâce au terminal (ou moniteur série). Pendant l'exécution du programme en mémoire sur l'Arduino, il est possible d'établir une communication avec l'ordinateur tant que la connexion est active (via un câble USB, par exemple). [25]

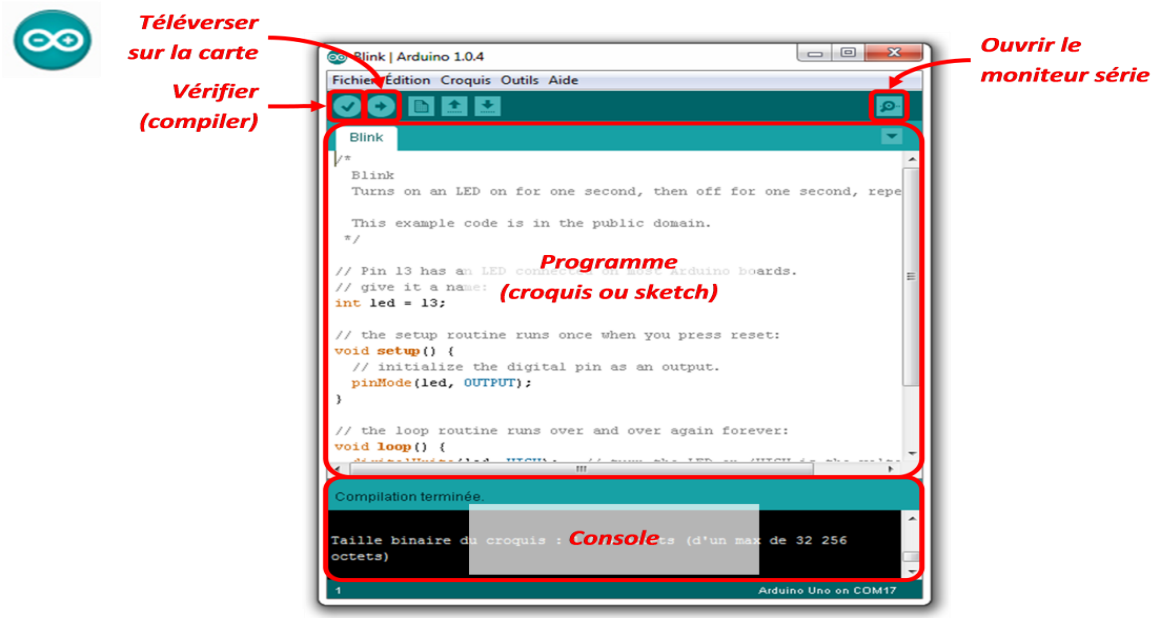


Figure 3- 8 : Logiciel arduino IDE

4 Logiciel de simulation

Pour simuler notre projet on va utiliser le logiciel Fritzing.

4.1 Fritzing

Fritzing est un logiciel complet et avancé développé dans le but d'aider les ingénieurs et les artistes à concrétiser leurs projets et leurs idées en créant des prototypes fonctionnels. Ce programme a été conçu comme un outil d'apprentissage, permettant aux utilisateurs d'apprendre à concevoir et à utiliser des cartes de circuits imprimés ainsi que d'autres composants électroniques. Dans la fenêtre principale de Fritzing, il est possible de visualiser le circuit virtuel en cours de construction, avec la possibilité de passer entre trois modes de vue : "Breadboard" (planche à pain), "Schematic" (schématique) et "PCB View" (vue PCB). Le mode "Breadboard" est le point de départ où nous pouvons créer un circuit qui simule la réalité, ce qui permet de prévenir les erreurs lors du passage du projet de l'état virtuel à un objet physique.

Fritzing dispose d'une bibliothèque complète de composants que nous pouvons simplement glisser-déposer dans notre projet. Tous les composants disponibles sont organisés par catégories. De plus, grâce à l'inspecteur de composants, il est possible de visualiser et de modifier les informations spécifiques à chaque composant du circuit. [26]

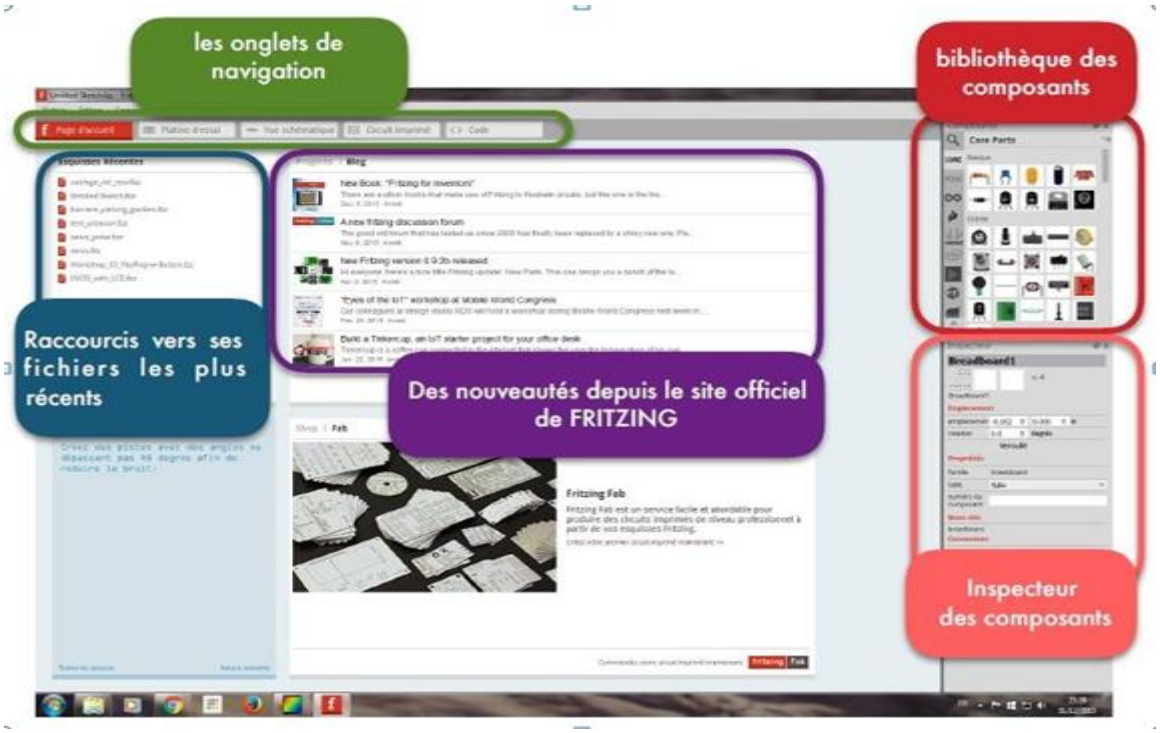


Figure 3- 9: Page d'accueil du logiciel Fritzing. **[27]**

5 Clavier numérique 4x4: (Keypad Module)

Le clavier joue un rôle essentiel dans un système de microcontrôleur, car il permet de définir les performances des fonctions à exécuter, de saisir des données et d'interagir avec la machine. Il est conçu avec une disposition matricielle des touches qui permet d'exploiter de manière efficace les broches du microcontrôleur. Grâce à cette configuration, les 16 touches peuvent être mappées en utilisant seulement 8 broches de données du microcontrôleur, ce qui simplifie grandement la programmation et facilite sa mise en œuvre. De plus, sa faible épaisseur lui permet d'être installé de manière pratique avec n'importe quel appareil. [28]

Figure 3- 10 :4x4 Key pad Module

6 La serrure électromagnétique 12v

la serrure électromagnétique a solénoïde 12v a une cosse avec une coupe inclinée et bon support de montage .il s'agit essentiellement d'une serrure électronique a électro-aimants, conçue pour une armoire de base un coffre-fort ou une porte .lorsque une tension de 9 à 12 VDC est appliquée la cosse s'enclenche pour ne pas dépasser et la porte peut être ouverte.il n'utilise aucun puissance dans cette état .Il est très facile à installer pour les système de verrouillage de porte automatique comme la serrure de la porte électrique avec le panneau de montage.

Figure 3- 11: Serrure électromagnétique 12v

- Tension de fonctionnement : 12 VDC.
- Temps de verrouillage : 1 seconde.
- Courant d'entrée : 0.4A ; DC 12V.
- Démentions : longueur 27 mm ; largeur 15mm ; hauteur 17mm ; langueur de la langue 7mm hauteur de la langue -10mm.
- Langueur de câble : 120mm. [29]

7 Circuit et composant

Le schéma de **La figure (3.12)** représente la configuration générale de notre projet et la connexion avec tous les périphériques de la maquette en utilisant le logiciel Fritzing.

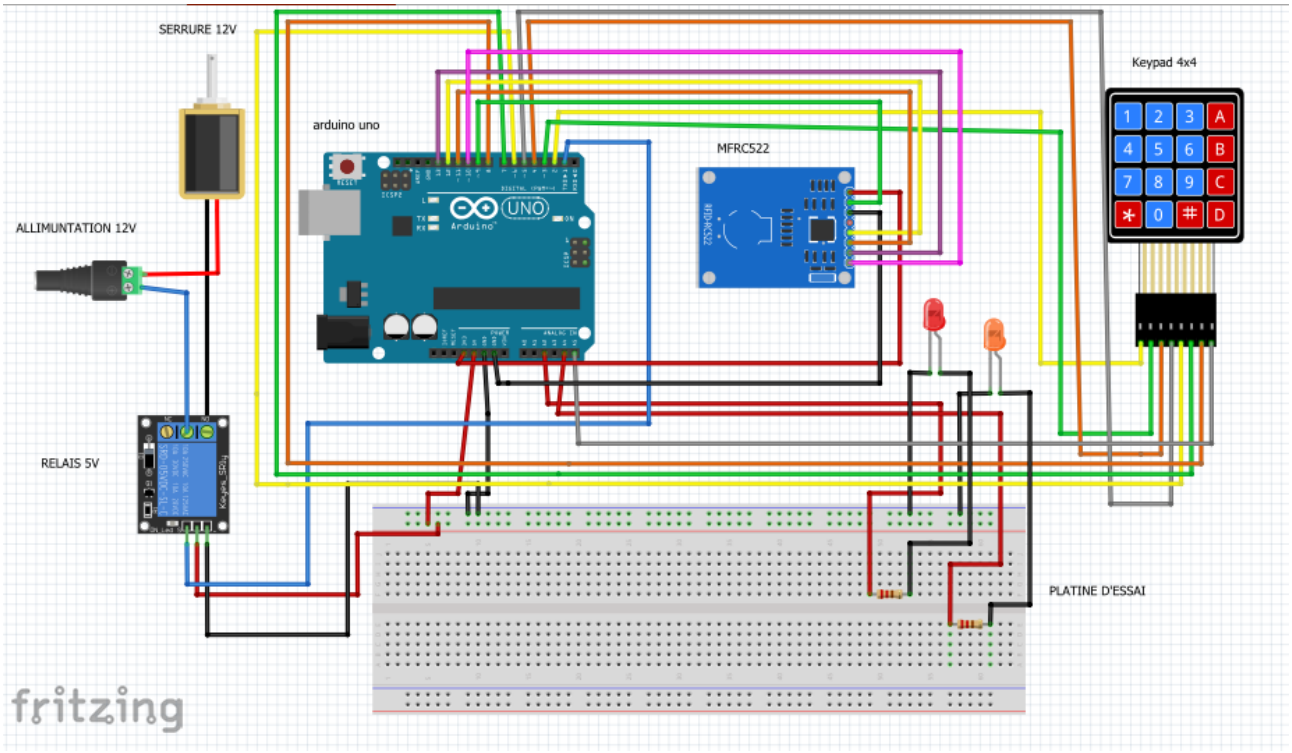


Figure 3- 12: Le schéma général de notre système

8 Les programmes de réalisations :

Dans ce chapitre, nous avons développé quatre programmes qui sont utilisés pour simuler une attaque et une contre-attaque.

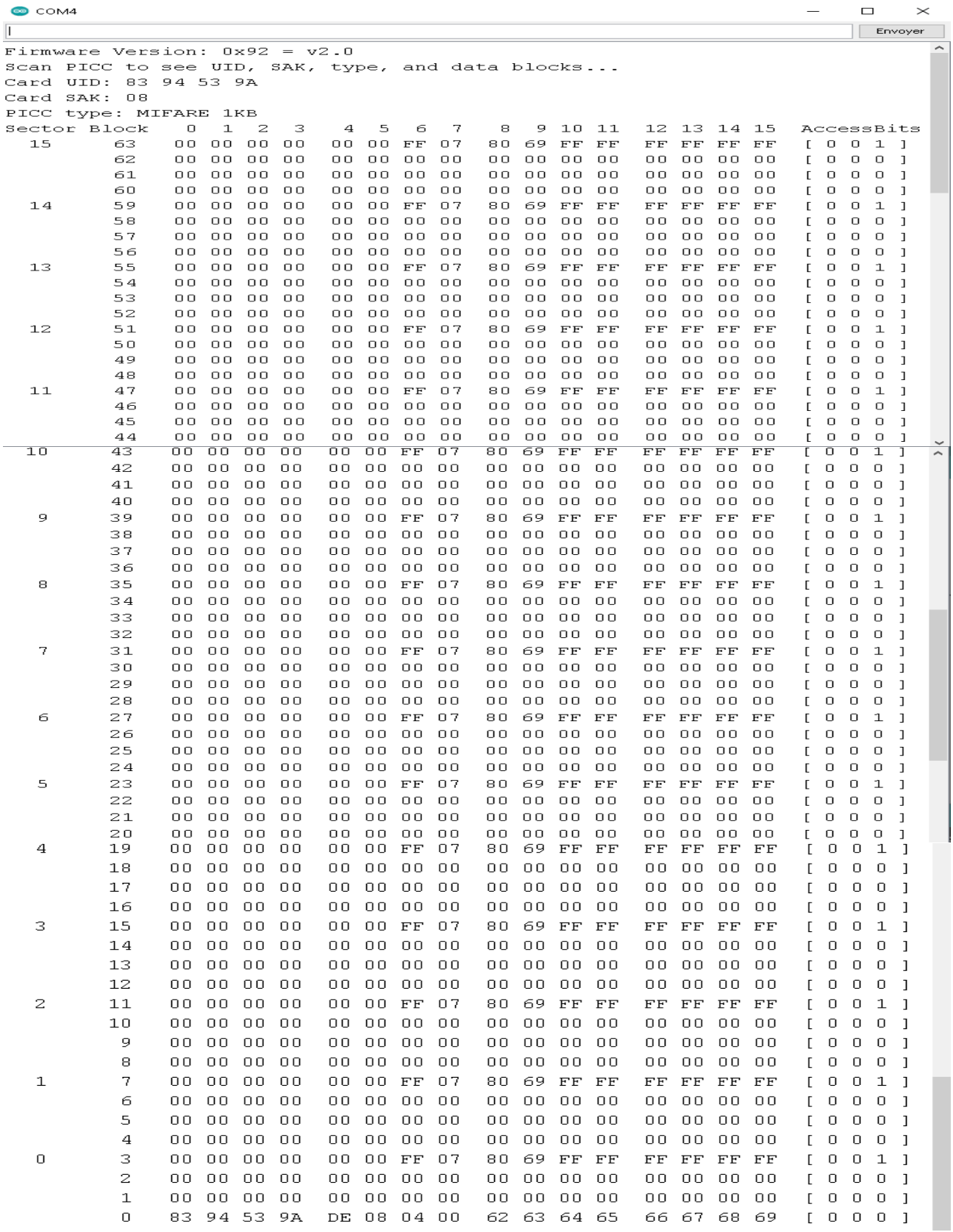
De nombreuses industries utilisent la technologie des cartes RFID comme moyen de contrôle d'accès. Ces cartes RFID offrent une commodité et une efficacité accrues par rapport aux méthodes traditionnelles telles que les clés. Cependant, la plupart des implémentations de ces cartes présentent des vulnérabilités en matière de sécurité car elles ne sont pas sécurisées contre les attaques physiques.

On a pu simuler le dispositif de l'attaquant en utilisant un Arduino et un module MFRC522, avec le code dump, on a facilement lu toutes les données de la carte. Cela signifie qu'un vrai attaquant peut cloner la carte facilement et la réutiliser.

- **Le premier code :**

Le premier programme, appelé "**Code Dump info**", est utilisé pour lire les données de la carte. Nous avons simulé ce code pour représenter le comportement d'un attaquant.

Résultat de premier code :



- **Deuxième code :**

Le deuxième programme, appelé "**Code de chiffrement de la clé**", concerne le chiffrement de la clé. Dans le cas de la carte Mifare Classic 1K, sa clé de chiffrement par défaut est « FFFFFFFFFFFF ». À l'aide de notre code, nous avons réussi à chiffrer la carte en utilisant une nouvelle clé secrète que nous avons choisie, à savoir « AAAAAAAAAAAA ».

- **Troisième code :**

Le troisième programme, intitulé **"Code d'écriture de donnée"**, concerne l'écriture des données. Dans ce code, nous avons choisi le bloc 60 situé dans le secteur 15 pour y écrire notre mot clé choisi, qui est « AFAF ». Nous avons choisi le bloc 60 qui est situé dans les derniers blocs afin de prévenir les attaques telles que la brute force.

La probabilité de déchiffrer ce bloc est calculée comme suit :$(1\times100 / (15^{12} + 15^{11} + ... + 15^{0}) \times 15)$ %

Voici quelques informations pour mieux comprendre le calcul :

- La clé de chiffrement par défaut est représentée par 12 chiffres hexadécimaux (FFFFFFFFFFFF).
- En notation hexadécimale, la lettre F correspond au chiffre 15.
- Le nombre 15 correspond au nombre total de secteurs (allant de 0 à 15).

- **Le dernier code :**

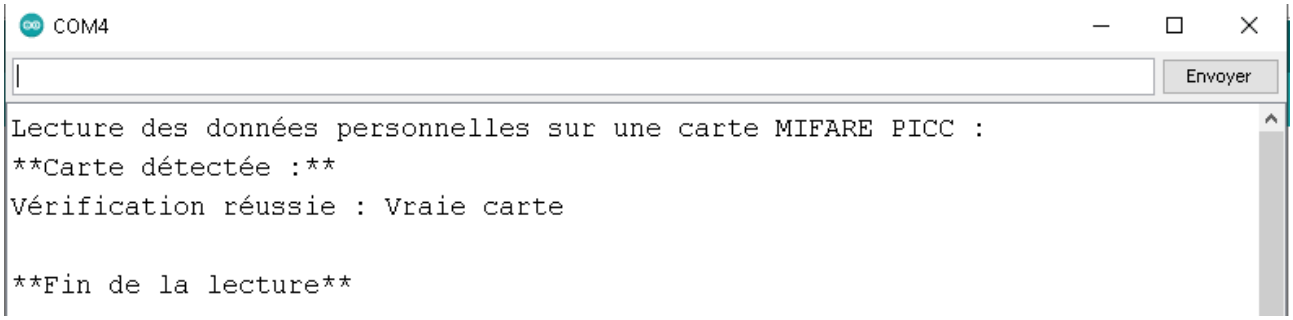
Le dernier programme, appelé **"Code d'authentification"**, concerne le processus d'authentification. Il vérifie si l'ID de la carte correspond à l'ID de notre carte Mifare Classic 1K. Ensuite, il utilise notre clé de chiffrement spéciale que nous avons introduite pour déchiffrer le secteur 15. Il vérifie également si le mot-clé dans le bloc 60 est identique à notre mot-clé (AFAF).

Grâce à cette méthode, nous garantissons une sécurité totale pour notre système en protégeant contre les attaques physiques telles que : (le clonage, le spoofing et le brute force).

- Si toutes les étapes sont vérifiées avec succès, notre système ouvrira l'accès. Sinon, il détectera qu'il s'agit d'une fausse carte et émettra une alerte.

9 Résultat de réalisation :

- **Carte mifare classic 1k (cartes authentiques)**



Le résultat nous a indiqué que la carte est authentique

- **Fausse carte : (coloning)**

```
**Carte détectée :**
Échec de l'authentification : Timeout in communication.
Vérification échouée : Fausse carte
```

Le résultat nous a indiqué que la carte est fausse

- **Carte non enregistré :**

```
**Carte détectée :**
Carte non valide

**Fin de la lecture**
```

Le résultat nous a indiqué que la carte est non enregistrée

<u>Deuxième méthode de vérification :</u>

La deuxième méthode d'accès du système de contrôle d'accès on utilise un clavier et un code pour déverrouiller la porte. L'utilisateur entre le code sur le clavier, puis le système vérifie la validité du code. Si le code est correct, la porte s'ouvre. En cas d'entrée incorrecte, le système émet un avertissement visuel pour signaler une erreur. Cette méthode offre une alternative pratique et sécurisée.

Résultat de clavier :

```
6666
Code d'accès correct : Ouverture de l'accès
```

Résultat code d’accès correct

10 Conclusion

En conclusion, ce chapitre présente notre proposition de solution de sécurité pour la carte Mifare Classic 1K, en incluant l'ajout d'une clé mécanique et d'un clavier à notre système basé sur la carte Arduino et la technologie RFID. Nous avons effectué une analyse approfondie des travaux existants dans le domaine, évalué différentes approches pour renforcer la sécurité des cartes RFID, et détaillé notre méthode de chiffrement spécifique. De plus, nous avons réalisé une expérimentation afin de mesurer l'efficacité de notre solution, et les résultats obtenus ont confirmé la validité de notre proposition. Ces avancées constituent une base solide pour nos recherches futures dans le domaine de la sécurité des systèmes embarqués.

Conclusion Générale

11 Conclusion Générale :

Ce mémoire a exploré les problèmes de sécurité dans les systèmes embarqués, en se concentrant sur les attaques physiques et en proposant une solution de protection basée sur une double vérification. Nous avons mis en évidence l'importance croissante des systèmes embarqués dans notre vie quotidienne, ainsi que leurs caractéristiques principales et leur architecture. Cependant, cette ubiquité des systèmes embarqués a également entraîné une augmentation des risques de sécurité.

Dans le premier chapitre, nous avons examiné les concepts fondamentaux de la sécurité, tels que la confidentialité, l'intégrité et la disponibilité, en soulignant les différentes attaques auxquelles les systèmes embarqués sont confrontés. Ces attaques comprennent l'utilisation de clés de cryptographie faibles, la réutilisation de codes et de composants non sécurisés, ainsi que d'autres sources potentielles d'attaques. Il est crucial de comprendre ces vulnérabilités afin de développer des mesures de protection efficaces.

Le deuxième chapitre s'est concentré sur la carte à puce, un composant clé des systèmes embarqués. Nous avons examiné les différentes familles et types de cartes à puce, en mettant l'accent sur la technologie RFID. Nous avons également analysé les composants spécifiques des cartes RFID, en accordant une attention particulière à la carte à puce RFID Mifare Classic 1K et aux types d'attaques auxquels elle est exposée. Cette exploration a permis de mettre en évidence les vulnérabilités potentielles des cartes à puce et l'importance de renforcer leur sécurité.

Dans le troisième chapitre, nous avons présenté une proposition de solution spécifique pour renforcer la sécurité de la carte Mifare Classic 1K, cette proposition de solution, qui intègre une clé mécanique, un clavier et la technologie RFID, offre une approche prometteuse pour renforcer la sécurité de ces systèmes. Les résultats de l'expérimentation confirment l'efficacité de cette solution et ouvrent la voie à de futures recherches dans le domaine de la sécurité des systèmes embarqués.

En conclusion, il est crucial de reconnaître les vulnérabilités des systèmes embarqués et de la technologie RFID, et d'adopter des mesures de sécurité adéquates pour protéger les données personnelles, financières et sensibles. Une approche collaborative impliquant les fabricants, les développeurs, les chercheurs en sécurité et les régulateurs est nécessaire pour relever les défis de sécurité posés par ces technologies. En restant attentifs aux développements technologiques et en mettant en œuvre des solutions de sécurité innovantes, nous pouvons garantir une utilisation sûre et

sécurisée des systèmes embarqués et de la technologie RFID dans un monde de plus en plus interconnecté.

Annexes :

- **Premier code : (lecteur de donnée)**

```
#include <SPI.h>
#include <MFRC522.h>

#define RST_PIN         9          // Configurable, see typical
pin layout above
#define SS_PIN          10         // Configurable, see typical
pin layout above

MFRC522 mfrc522(SS_PIN, RST_PIN);  // Create MFRC522 instance

void setup() {
      Serial.begin(9600);       // Initialize serial communications
with the PC
      while (!Serial);          // Do nothing if no serial port is
opened (added for Arduinos based on ATMEGA32U4)
      SPI.begin();              // Init SPI bus
      mfrc522.PCD_Init();       // Init MFRC522
      delay(4);                       // Optional delay. Some
board do need more time after init to be ready, see Readme
      mfrc522.PCD_DumpVersionToSerial();     // Show details of PCD
- MFRC522 Card Reader details
      Serial.println(F("Scan PICC to see UID, SAK, type, and data
blocks..."));
}

void loop() {
      // Reset the loop if no new card present on the
sensor/reader. This saves the entire process when idle.
      if ( ! mfrc522.PICC_IsNewCardPresent()) {
            return;
      }

      // Select one of the cards
      if ( ! mfrc522.PICC_ReadCardSerial()) {
            return;
      }

      // Dump debug info about the card; PICC_HaltA() is
automatically called
      mfrc522.PICC_DumpToSerial(&(mfrc522.uid));
}
```

- **Deuxieme code : (chiffrement de la clé)**

```
#include <MFRC522.h>
#include <SPI.h>

#define SS_PIN 10
#define RST_PIN 9

MFRC522 mfrc522(SS_PIN, RST_PIN);

void setup() {
  Serial.begin(9600);
  SPI.begin();
  mfrc522.PCD_Init();
  Serial.println("Scannez la carte pour changer les clés de
chiffrement de tous les secteurs...");
}

void loop() {
  if (mfrc522.PICC_IsNewCardPresent() &&
mfrc522.PICC_ReadCardSerial()) {
    Serial.println("Carte détectée!");

    // Changer la clé de chiffrement pour chaque secteur
    for (byte sector = 0; sector < 16; sector++) {
      MFRC522::MIFARE_Key key;
      byte newKey[6] = {0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF}; // La
clé par défaut de l'usine de fabrication !!!

      for (byte i = 0; i < 6; i++) {
        key.keyByte[i] = newKey[i];
      }
      // Authentifier avec la clé actuelle
      if
(mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A, sector
* 4, &key, &(mfrc522.uid)) == MFRC522::STATUS_OK) {
        // Changer la clé de chiffrement
        mfrc522.MIFARE_SetAccessBits(sector * 4, 0xAA, 0xAA, 0xAA,
0xAA);//Notre Nouvelle clé de chiffrement pour tout les
secteurs!!!
        Serial.println("Clé de chiffrement changée avec succès
pour le secteur " + String(sector));
      } else {
        Serial.println("Échec du changement de clé de chiffrement
pour le secteur " + String(sector));
      }
      mfrc522.PICC_HaltA(); }}}
```

- **Troisième code : (écriture de donnée)**

```
- #include <SPI.h>
- #include <MFRC522.h>
-
- #define RST_PIN         9
- #define SS_PIN          10
-
- MFRC522 mfrc522(SS_PIN, RST_PIN);
-
- void setup() {
-   Serial.begin(9600);
-   SPI.begin();
-   mfrc522.PCD_Init();
-   Serial.println(F("Écriture du mot  Clé\"AFAF\" dans le bloc 60
  d'une carte MIFARE Classic 1K :"));
- }
-
- void loop() {
-   MFRC522::MIFARE_Key key;
-   for (byte i = 0; i < 6; i++) key.keyByte[i] = 0xAA;//Notre clé
  de chiffrement
-
-   byte block = 4;
-   byte len = 18;
-   MFRC522::StatusCode status;
-
-   if (!mfrc522.PICC_IsNewCardPresent()) {
-     return;
-   }
-
-   if (!mfrc522.PICC_ReadCardSerial()) {
-     return;
-   }
-
-   Serial.println(F("**Carte détectée :**"));
-
-   status =
  mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A, block,
  &key, &(mfrc522.uid));
-   if (status != MFRC522::STATUS_OK) {
-     Serial.print(F("Échec de l'authentification : "));
-     Serial.println(mfrc522.GetStatusCodeName(status));
-     return;
-   }
-
-   byte buffer[18];
-   for (uint8_t i = 0; i < len; i++) {
-     if (i < 4) {
-       buffer[i] = 'A';
-     } else {
```

```
-         buffer[i] = 'F';
-       }
-     }
-
-     status = mfrc522.MIFARE_Write(block, buffer, len);
-     if (status != MFRC522::STATUS_OK) {
-       Serial.print(F("Échec de l'écriture : "));
-       Serial.println(mfrc522.GetStatusCodeName(status));
-       return;
-     }
-
-     Serial.println(F("Le mot \"AFAF\" a été écrit avec succès dans
   le bloc 4 de la carte."));
-
-     Serial.println(F("\n**Fin de l'écriture**\n"));
-
-     delay(1000);
-     mfrc522.PICC_HaltA();
-     mfrc522.PCD_StopCrypto1();
- }
```

Dernier code : code authentification

```
- #include <SPI.h>
- #include <MFRC522.h>
- #include <Wire.h>
- #include <Keypad.h>
-
- #define RST_PIN 9
- #define SS_PIN 10
-
- #define LED_TRUE A0
- #define LED_FALSE A2
- #define LED_NOT_REGISTERED A4
-
- MFRC522 mfrc522(SS_PIN, RST_PIN);
-
- const byte ROWS = 4; // Quatre rangées
- const byte COLS = 4; // Quatre colonnes
- char keys[ROWS][COLS] = {
-   {'1','2','3','A'},
-   {'4','5','6','B'},
-   {'7','8','9','C'},
-   {'*','0','#','D'}
- };
- byte rowPins[ROWS] = {2, 3, 4, 5}; // Connectez les broches de
   rangée du clavier aux broches A1, A2, A3 et A4 de votre Arduino
- byte colPins[COLS] = {6, 7, 8, A5}; // Connectez les broches de
   colonne du clavier aux broches A5, 8, 7 et 6 de votre Arduino
-
- Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS,
   COLS);
-
```

```
- // Définir les valeurs UID pour chaque carte
- byte card1UID[] = {0x16, 0x74, 0xC8, 0x49};
- byte card2UID[] = {0xC3, 0xBA, 0xD6, 0xAA};
- byte card3UID[] = {0x86, 0x7F, 0x34, 0x1F};
-
- String accessCode = ""; // Variable pour stocker le code d'accès
-
- void setup()
- {
-   Serial.begin(9600);
-   SPI.begin();
-   mfrc522.PCD_Init();
-
-   pinMode(LED_TRUE, OUTPUT);
-   pinMode(LED_FALSE, OUTPUT);
-   pinMode(LED_NOT_REGISTERED, OUTPUT);
-
-   Serial.println(F("Lecture des données personnelles sur une
  carte MIFARE PICC :"));
- }
-
- void loop()
- {
-   MFRC522::MIFARE_Key key;
-   for (byte i = 0; i < 6; i++)
-     key.keyByte[i] = 0xAA;
-
-   byte block;
-   byte len;
-   MFRC522::StatusCode status;
-
-   if (mfrc522.PICC_IsNewCardPresent() &&
  mfrc522.PICC_ReadCardSerial())
-   {
-     Serial.println(F("**Carte détectée :**"));
-
-     bool validCard = false;
-     bool authentic = false;
-
-     // Vérifier si l'UID de la carte existe dans la liste
  fournie
-     if (checkUID(mfrc522.uid.uidByte, card1UID) ||
  checkUID(mfrc522.uid.uidByte, card2UID) ||
  checkUID(mfrc522.uid.uidByte, card3UID))
-     {
-       validCard = true;
-
-       byte buffer[18];
-       block = 60;
-       len = 18;
-
```

```
-         status =
   mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A, block,
   &key, &(mfrc522.uid));
-         if (status != MFRC522::STATUS_OK)
-         {
-           Serial.print(F("Échec de l'authentification : "));
-           Serial.println(mfrc522.GetStatusCodeName(status));
-           Serial.println(F("Vérification échouée : Fausse
   carte"));
-           digitalWrite(LED_FALSE, HIGH);
-           delay(2000);
-           digitalWrite(LED_FALSE, LOW);
-           return;
-         }
-
-         status = mfrc522.MIFARE_Read(block, buffer, &len);
-         if (status != MFRC522::STATUS_OK)
-         {
-           Serial.print(F("Échec de la lecture : "));
-           Serial.println(mfrc522.GetStatusCodeName(status));
-           Serial.println(F("Erreur de lecture"));
-           delay(2000);
-           return;
-         }
-
-         String data = "";
-         for (uint8_t i = 0; i < len; i++)
-         {
-           data += (char)buffer[i];
-         }
-
-         // Vérifier si le mot à l'intérieur est "AFAF"
-         if (data.equals("AFAF"))
-         {
-           authentic = true;
-         }
-       }
-
-       if (!validCard)
-       {
-         Serial.println(F("Carte non valide"));
-         digitalWrite(LED_NOT_REGISTERED, HIGH);
-         delay(2000);
-         digitalWrite(LED_NOT_REGISTERED, LOW);
-       }
-       else if (authentic)
-       {
-         Serial.println(F("Vérification réussie : Vraie carte"));
-         digitalWrite(LED_TRUE, HIGH);
-         delay(2000);
-         digitalWrite(LED_TRUE, LOW);
-       }
-       else
```

```
-      {
-        Serial.println(F("Vérification échouée : Fausse carte"));
-        digitalWrite(LED_FALSE, HIGH);
-        delay(2000);
-        digitalWrite(LED_FALSE, LOW);
-      }
-
-      Serial.println(F("\n**Fin de la lecture**\n"));
-    }
-    else if (keypad.getKeys())
-    {
-      for (int i = 0; i < keypad.numKeys(); i++)
-      {
-        char key = keypad.key[i].kchar;
-        if (key >= '0' && key <= '9')
-        {
-          accessCode += key;
-          Serial.print(key); // Afficher le chiffre dans le
   moniteur série
-        }
-        else if (key == '#')
-        {
-          Serial.println(); // Aller à la ligne dans le moniteur
   série
-          if (accessCode.equals("6666")) // Remplacez "1234" par
   votre propre code d'accès
-          {
-            Serial.println(F("Code d'accès correct : Ouverture de
   l'accès"));
-            digitalWrite(LED_TRUE, HIGH);
-            delay(2000);
-            digitalWrite(LED_TRUE, LOW);
-          }
-          else
-          {
-            Serial.println(F("Code d'accès incorrect"));
-            digitalWrite(LED_FALSE, HIGH);
-            delay(2000);
-            digitalWrite(LED_FALSE, LOW);
-          }
-
-          accessCode = ""; // Réinitialiser le code d'accès
-        }
-      }
-    }
-
-    delay(1000);
-    mfrc522.PICC_HaltA();
-    mfrc522.PCD_StopCrypto1();
-  }
-
-  bool checkUID(byte* uid, byte* targetUID)
-  {
```

```
-    for (byte i = 0; i < 4; i++)
-    {
-      if (uid[i] != targetUID[i])
-      {
-        return false;
-      }
-    }
-    return true;
-  }
```

12 Bibliographie

[1] R. Lekhal, «Conception d'un système embarqué pour le suivi préventif d'un château d'eau,» Biskra, 2019.

[2] R. canacho, «online,» 17 juin 2021. [En ligne]. Available: https://fr.parasoft.com/blog/what-is-an-embedded-system.

[3] T. Lassaad, «Support de cours systèmes embarqués, institut supérieur des études technologiques des,» Gabès, 2015.

[4] «Agixis,» vendredi 1 février 2019. [En ligne]. Available: https://www.agixis.com/focus-lelectronique-embarquee/.

[5] A. Manar El Houda et C. Nour El Houda, «Conception et réalisation d'un système embarqué pour mesurer les paramètres d'une ligne téléphonique,» Blida, 2019.

[6] 2023. [En ligne]. Available: https://www.clicours.com/memoire-online-les-problemes-de-securite-dans-les-systemes-embarques/.

[7] *Introduction à la sécurité des systèmes embarqués introduction à la sécurité des systèmes embarqués,* 2007.

[8] [En ligne]. Available: https://www.sfrbusiness.fr/room/securite/differents-types-menaces-informatiques-entreprises.html.

[9] M. Bada, *Les Problèmes De Sécurité Dans Les Systèmes Embarqués,* Batna, Université de Batna, 2012.

[10] *Attaques par canaux caché.,* université du Québec à Montréal, 2019.

[11] C. Clavier, *De la sécurité physique des cryptosystèmes embarqués,* Versailles SaintQuentin-en-Yvelines, Université de Versailles SaintQuentin-en-Yvelines, Laboratoire de recherche en informatique, 2007.

[12] X. Kauffmann-Tourkestanky, *Analyses sécuritaires de code de carte à puce sous attaques physiques simulées,* université d'Orléans, 2012.

[13] 24 Janvier 2023. [En ligne]. Available: https://www.redsen.com/transformation-digitale/technologie-rfid-en-6-points/?fbclid=IwAR24Ho3DlwRU0G8micjRrBogZDQAdKp8UCTIXQZKKjsT-1jV9hBwAsshRIs .

[14] «CIPAM Traçabilité & solution connectées,» [En ligne]. Available: https://www.cipam.com/a-propos/solutions/rfid.

[15] B. M. &. B. YAAKOUB, 2013/2014. [En ligne]. Available: https://www.academia.edu/22452132/Identification_par_radio_Fréquences_RFID?fbclid=IwAR170e7FtSBXDY4eQdxI3TkbRYpkfA_ryFqddr9YiU7CSAN-MP8jhejUz88.

[16] 3 mars 2021. [En ligne]. Available: https://www.rfidfuture.com/fr/about-rfid-cards.html.

[17] [En ligne]. Available: https://www.eurequat-algerie.com/wp-content/uploads/2019/12/Carte-à-puce-.pdf].

[18] I. TC, «TAG RFID et ses failles de sécurité,» 30 octobre 2020. [En ligne]. Available: https://medium.com/insa-tc/tag-rfid-et-ses-failles-de-sécurité-6dcd90047393.

[19] C.Fréou et A.Grimault, « Découverte des cartes Aduino ,» [En ligne]. Available: http://www.techmania.fr/arduino/Decouverte_arduino.pdf.

[20] «Module RFID RC 522,» 2016-2020. [En ligne]. Available: https://www.smart-cube.biz/produit/module-rfid-rc522.

[21] « Tricartes MIFARE classic ® 1K NXP EV1 ,» [En ligne]. Available: https://www.barcoda.fr/126578-tri-cartes-blanches-rfid-mifare-classic-1k-nxp.html.

[22] «Module RFID RC 522 lecteur RFID,» [En ligne]. Available: https://www.moussasoft.com/product/module-rfid-rc522-lecteur-rfid.

[23] «What is RFID ? How it works ? Interface RC 522 RFID module with Arduino ,» [En ligne]. Available: https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/.

[24] S. Bouzefrane, *La technologie RFID / NFC,* Laboratoire CEDRIC – CNAM.

[25] « L'IDE Arduino ,» [En ligne]. Available: https://arduino.blaisepascal.fr/presentation/logiciel/.

[26] « Fritzing,» [En ligne]. Available: https://www.01net.com/telecharger/windows/Multimedia/creation_graphique/fiches/149413.

[27] [En ligne]. Available: https://disciplines.actoulouse.fr/sii/sites/sii.disciplines.actoulouse.fr/files/ressources/didactici .

[28] «Clavier matriciel ,» 2023. [En ligne]. Available: https://www.dondeleo.com/fr/prodotto/clavier-matriciel-4x4-16-touches-pour -arduino/.

[29] « La serrure électromagnétique ,» [En ligne]. Available: https://www.micro-planet.ma/produit/serrure-electromagnetique-12v/.

[30] [En ligne]. Available: https://www.avast.com/fr-fr/c-what-is-the-internet-of-things.