



La carte : types et utilisations

Ahmed ZELLOU

Université Mohammed V-Agdal

Zellou@um5a.ac.ma

Journée Carte : 12 mars 2009

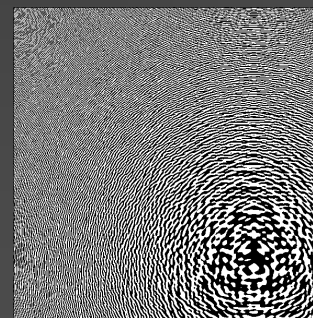
La Carte de l'identification à l'authentification

Plan

- La carte simple PVC
- La carte à piste magnétique
- La carte à puce
- La carte Radio Frequency Identification
- La carte MIkron FARE-collection System
- Comparaison
- Quelques Utilisations

Simple PVC

- Le support de toutes les technologies.
- Elle supporte toutes technologies à base d'impression (code à barre simple ou bidimensionnel).
- La personnalisation logique de la carte.
- Peut comporter un hologramme pour éviter la contrefaçon.



Carte Magnétique

- Issus d'une technologie du début du 20ème siècle, l'enregistrement et la lecture magnétique sont encore très utilisés de nos jours.
- Coût bas et mise en œuvre aisée : lecteurs magnétiques onéreux.
- Technologie à contact fiable et peut être utilisée parallèlement avec un code à barre.
- Le principe de l'enregistrement magnétique repose sur la magnétisation de très petites zones de la bande.
- L'enregistrement/écriture s'effectue par une tête magnétique.
- La densité d'enregistrement est mesurée en bpi.
- Les données sont toujours encadrées par un caractère start, un caractère end et un caractère sep pour séparer les différents champs de données.
- Un contrôle de parité est utilisé pour la gestion d'erreurs.

Sécurité

- Nombreuses utilisations :
 - Tickets avec une bande magnétique (métro, bus, train, parking,...),
 - Cartes avec une piste magnétique (carte bleue, carte de fidélité, carte d'abonnement, carte de contrôle d'accès,...).
- La lecture et l'écriture sont entièrement libres (contrairement aux cartes à puce qui possèdent des zones où l'écriture et la lecture sont interdites).
- Aucun moyen sûr pour protéger physiquement les données enregistrées sur un support magnétique.
- Mesures de sécurité
 - Sécuriser l'application utilisant ce support ;
 - Contrôler l'authenticité de la carte en temps réel et on-line ;
 - Crypter les données sensibles enregistrées sur le support ;
 - Coupler l'utilisation de la carte avec un code secret.

Carte à puce

- Une carte en matière plastique portant un circuit intégré capable de contenir de l'information.
- Le circuit intégré (la puce) peut contenir
 - Un microprocesseur 8 bits à 4 MHz,
 - 6 à 32 Ko de mémoire morte,
 - 256 à 2048 octets de mémoire vive,
 - 1 à 32 Ko d'EEPROM,
- Fournit des moyens d'effectuer des transactions d'une manière flexible, bloquée, standard avec une intervention humaine minimale (peut fournir l'authentification forte par SSO), USB.
- La personnalisation physique / logique de la carte.

Catégories

- Trois types
 - les cartes à mémoire (comme les télécartes) ;
 - les cartes à logique câblée (utilisées dans certains décodeurs de chaîne payante) ;
 - les cartes à microprocesseurs (mono-applicatives, multi-applicatives)
- Accessibilité
 - Par contact avec des électrodes de cuivre.
 - Sans contact: par radiofréquence à courte ou à moyenne portée, via une antenne interne.
 - par une combinaison des deux précédentes : on parle alors de cartes Avec et Sans Contact (ASC).

Sécurité

- Un programme de codage (décodage) et/ou un code (mot de passe) dans la puce, inaccessibles de l'extérieur, sont garants d'une bonne sécurité (au sens bancaire).
- Utilisée principalement comme
 - moyens d'identification personnelles : carte d'identité, badge d'accès aux bâtiments, carte d'assurance maladie, carte SIM,..
 - moyen de paiement : carte bancaire, porte-monnaie électronique,..
 - Preuve d'abonnement à des services prépayés : carte de téléphone, titre de transport,..

Radio Frequency Identification

- RFID est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (*RFID tag*).
- Les radio-étiquettes sont de petits objets discrets (taille réduite, masse négligeable et coût minime) qui peuvent être collées ou incorporées dans des objets/produits/organes.
- Les radio-étiquettes comprennent une antenne associée à une puce électronique pour recevoir et répondre aux requêtes radio émises depuis l'émetteur-récepteur 200m.
- Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires.

Catégories

- Trois types
 - Marqueurs passifs (pas d'énergie, 10m).
 - Marqueurs actifs qui diffuse le signale (200 m).
 - Marqueurs semi-actifs agissent comme des étiquettes passives au niveau communication, leur batterie leur permet d'enregistrer des données.
- Utilisée principalement pour identifier :
 - des objets comme avec un code à barres (étiquette électronique)
 - des personnes en étant intégrée dans les passeports, carte de transport, carte de paiement (carte sans contact).

Sécurité

- Une émission active signale à tous la présence des marqueurs et pose des questions quant à la sécurité.
- Possibilité d'atteinte à la vie privée, toute personne recevant ces ondes, pourrait localiser ou même identifier cet objet/individu.
- L'environnement métallique constitue un obstacle qui diminue la distance possible de communication.
- Les communications sont brouillées lorsque plusieurs marqueurs se trouvent dans le champ d'un même lecteur (Collision), méthodes d'anticollision.
- Génération de signaux pouvant s'avérer dangereux pour la santé (cancers, ...) ou interférant avec le fonctionnement des appareils bio-médicaux.

Mikron FARE-collection System

- MIFARE est une technologie de carte à puce sans contact très répandues dans le monde avec 500 millions de cartes et 5 millions de modules de lecteurs/encodeurs.
- La technologie est intégrée à la fois dans les cartes et dans les lecteurs/encodeurs.
- Sont des cartes mémoires disposant d'un numéro de série de 32/56 bits pré-encodé et d'un espace de stockage découpé en segments de données puis en blocs de données avec des mécanismes de sécurité simples.

Catégories

1. Les cartes Classiques

- faussement appelées Standard,
- respectent partiellement le standard ISO 14443A (couche 1-3).
- utilisent un protocole propriétaire (couche 4)
- utilisent un protocole de sécurité propriétaire pour l'authentification et le chiffrement.
- un numéro de série ou CSN de 32 bits
- La MIFARE Classic 1k offre 768 octets de stockage répartis sur 16 secteurs. Chaque secteur est composé de 3 blocs de 16 octets + un bloc de sécurité (protection d'accès par 2 clefs différentes).
- La MIFARE Classic 4k offre 3 k répartis sur 64 secteurs.
- Les secteurs sont gérés via des opérations de lecture/d'écriture de données ou d'incrément/décément de valeurs.

Catégories

2. Les cartes UltraLight

- Utilisent le même protocole mais sans la partie sécurité.
- La MIFARE UltraLight a 64 octets.
- Coût très bas fait qu'elle sert souvent de ticket jetable.
- Disposent de circuits intégrés applicatifs spécifiques et ont une capacité de calcul limitée.
- Utilisées essentiellement dans le transport, billetterie, portemonnaie électronique, gestion d'accès (physiques et logiques), gestion d'horaire, etc.

3. Les cartes MIFARE ProX et SmartMX

- Complètement conformes au standard l'ISO 14443A.
- à base de microprocesseur, la puce est programmée avec un logiciel dédié et un système d'exploitation.

Catégories

3. Les cartes MIFARE ProX et SmartMX

- Le microprocesseur est couplé à un coprocesseur spécialisé pour les calculs cryptographiques rapides (Triple DES, AES, RSA, etc).
- Capables d'exécuter des opérations complexes de façon sécurisée et rapide.
- Utilisée pour tous types d'applications nécessitant un haut niveau de sécurité.

4. MIFARE DESFire

- Une version spéciale de SmartMX.
- Idem MIFARE Standard (soit 4 ko de stockage répartis sur 16 zones) avec une plus grande flexibilité, une sécurité accrue avec du Triple DES et une communication plus rapide.
- Vendue pré-programmée avec DESFireOS.

Types d'utilisation

- Lecture du numéro de série
 - Concerne 80% de l'utilisation de Mifare en contrôle d'accès.
 - La lecture ne fait pas appel à la mémoire de la carte,
 - La lecture s'effectue sans aucun dispositif de sécurité, la duplication et le "replay attack" par N° de série est assez aisée, son utilisation est en recul.
- La lecture /écriture:
 - Utilisation complète de la mémoire (comme une clé USB), cette utilisation fait appel à des clés de sécurité.
 - Chaque fabricant peut livrer des lecteurs Mifare faisant appel à des clés ou des systèmes de protection différents.

Comparaison

	Coût unité	Coût encodeur/lecteur	Qte d'info.	Usage	Sécurité
PVC	1	X	X	X	X
Magn.	2	2	3*64 O	garde	Faible
A puce	10	1.2	2 à 4 Ko	-	Forte
RFID	10	1	4 Ko	+	Forte
MIFARE	10	1	4 Ko	+	Forte

Quelques Utilisations

Carte de paiement

- Un moyen de paiement sous forme de carte PVC, équipée d'une bande magnétique et/ou puce électronique qui permet :
 - le paiement d'achats et prestations de services, auprès de fournisseurs possédant un « terminal de paiement » pouvant lire la carte et connecté ou non à sa banque ou dans un appareil de distribution automatique ;
 - les retraits d'espèces aux distributeurs de billets ;
 - le télépaiement internet, etc.
- Non respect de la vie privée et données personnelles : Traçabilité
- Poids économique, 1350 milliards d'euros en europe en 2005.

Porte-monnaie électronique

- Un dispositif qui peut stocker de la monnaie à partir d'un dépôt bancaire et d'effectuer directement des paiements sur des terminaux de paiement.
- Se présente sous forme d'une carte à puce, mais le dispositif électronique peut s'installer sur une grande variété d'appareils comme par exemple des clés USB, des téléphones mobiles, etc.
- La vocation de ces dispositifs est :
 - ⑩ se simplifier la vie ;
 - ⑩ limiter le besoin de fournir des billets et des pièces de monnaie ;
 - ⑩ diminuer la très coûteuse gestion des pièces métalliques ;
 - ⑩ restreindre le risque sur les chèques ;
 - ⑩ profiter d'un moindre coût que celui de la carte bancaire.

Mon€o

- Le système français de porte-monnaie électronique.
- 300.000 cartes et plusieurs millions de transactions.
- Ses caractéristiques sont la rapidité et l'anonymat.
- Les montants concernés par les transactions sont de l'ordre de la petite monnaie : distributeur, automate, café, boulangerie, journal,...
- Le rechargement s'effectue sur des bornes spéciales et sur les terminaux de paiement électroniques.
- Moneo est géré par le consortium BMS Billetique Monétique Service qui regroupe dix banques françaises mais également la SNCF, la RATP et France Télécom.
- Avec l'arrivée de la carte BMS2 (sans contact), Moneo est devenue multi-services (cartes de cantine, carte de bibliothèque, badge d'accès,...).



Merci

