Programmation cartes à puces

Loïc Demange
loic.demange@etud.univ-paris8.fr

avec les notes de cours de Philippe Guillot

24/28 janvier 2021

Préliminaires

- 10 cours de 3h
- Trois rapports à rendre, un par projet (théorique)

Préliminaires

- 24/28 janvier - Contexte et introduction
- 31/4 février - Projet porte-monnaie (Calcul et EEPROM)
- 7/11 février - Projet porte-monnaie (ACID)
- 14/18 février - Projet porte-monnaie (Chiffrement)
- 21/25 février - Projet SIM (États)
- 28/4 mars - Projet SIM (Attaques temporelles)
- 7/11 mars - Projet SIM (Attaques par consommation)
- 14/18 mars - Projet RSA (Implémentation)
- 21/25 mars - Projet RSA (Interruptions)
- 28 mars/1 avril - Pause
- 4/8 avril - Projet RSA (Assembleur)

Contexte

Contexte historique

- Objectif : Remplacer les pièces de monnaie
- Application ciblée : carte téléphonique, porte monnaie, etc.

Contexte

Brevets fondateurs

- Roland Moréno 1974 - mémoire sécurisée
- Michel Ugon 1978 - ajout d'un microprocesseur

La cryptographie devient publique en parallèle (DES en 1974, Diffie-Hellman en 1976).

Contexte

Applications actuelles

- Téléphonie mobile (carte SIM)
- Carte bancaire
- TV à péage
- Transports
- etc.

Contexte

Guerre idéologique entre la France et les USA, menant à l'attaque des cartes TV à péage et menaçant l'avenir de la carte à puce.
Sauvé par la téléphonie mobile.

Contexte

Définition : Dispositif électronique fiable pour numériser et traiter des secrets.

Format :

- Carte de crédit
- Carte SIM (micro, nano, etc.)
- Clé USB

Marché :

- Télécom
- Banque
- Gouvernement
- Équipementiers
- Transport

Introduction

ATMega 163/328p reposant sur un microcontrôleur AVR, proposant plusieurs mémoires

- RAM : mémoire volatile (entre 1 et 2 Ko)
- EEPROM : mémoire non volatile accessible en lecture et écriture par le programme (entre 512 o et 1 Ko)
- Progmem (flash) : programmable par protocole physique (entre 16 et 32 Ko)

Introduction

Cycle de vie

- Développement logiciel/test
  Conception
  Compilation
- Production (fondeur)
  Programmation Progmem
- Personnalisation
- Vie chez l'utilisateur
- Destruction

Introduction

Norme ISO 7816-

- 1 : Caractéristiques techniques physiques
- 2 : Dimensions et emplacements des contacts
- 3 : Interface électrique et protocole de transmissions
- 4 : Organisation, sécurité des échanges et commandes
- 5 : Enregistrement des fournisseurs
- 6 : Éléments de données intersectoriels pour les échanges

Introduction

Étapes de communication avec la carte

- Initialisation ATR (Answer to Reset)
- Commande APDU (Application Protocol Data Unit)

Introduction

L'initialisation ATR consiste en l'envoi à la carte

- De l'octet représentant le protocole utilisé et le format d'E/S (ici, $0x3b$)
- D'une taille d'historique
- D'un historique (identité de la carte)

Introduction

Format de commande APDU à envoyer la carte : CLA INS P1 P2 P3 (ISO 7816-3 et 4)

- CLA : classe unique pour l'application
- INS : instruction (numéro de la commande)
- P1, P2 : paramètres supplémentaires
- P3 : taille des données transmises

Si c'est une commande entrante, on met les octets à transmettre après P3 (de taille P3).
Si c'est une commande sortante, la carte répondra des octets (de taille P3).

Dans les deux cas, la carte renvoie en premier lieu INS si la commande est correcte (acquittement).

Introduction

Réponse de la carte : status word (ISO 7816-3)

- 90 00 : fin normale
- 6E 00 : CLA inconnue
- 6D 00 : INS inconnu
- 6B 00 : P1, P2 incorrects
- 6C xx : P3 incorrect (taille), xx contient la taille correcte
- 6F 00 : commande inconnue

Introduction

Cycle de développement

- Développement et compilation (langage C, GCC)
- Programmation (AVRDUDE)
- Tests (SCAT)

TP

Objectifs du TP :

- Lire et comprendre le code du fichier hello.c.
- Ajouter une fonction sortir_data() qui permet de récupérer les données introduites par intro_data().