SÉRIE | EEA

Christian Tavernier

LES CARTES À PUCE

Théorie et mise en œuvre

2e édition

DUNOD

Christian Tavernier

LES CARTES À PUCE

Théorie et mise en œuvre

2e édition

DUNOD

TABLE DES MATIÈRES

Avant-propos 1

A

Description

1 • Présentation générale 5

1.1 Historique 5
1.2 Quelques chiffres 6
1.3 Une normalisation parfaite 7
1.4 Caractéristiques physiques et électriques des cartes à puce à contacts 11
1.5 Caractéristiques physiques et électriques des cartes à puce sans contact 28
1.6 Les différents types de cartes à puce (avec ou sans contact) 40

2 • Les cartes à mémoire ou cartes synchrones 45

2.1 Les anciennes cartes à mémoire OTPROM ou télécartes 45
2.2 Les cartes à mémoire I2C 53
2.3 Les cartes protégées à jetons 60
2.4 Les cartes à mémoire sécurisée 62
2.5 Les cartes à mémoire sans contact 70
2.6 Synthèse 75

3 • Les « vraies » cartes à puce ou cartes à microcontrôleur 77

3.1 Réponse au reset ou ATR 77
3.2 Le protocole $T = 0$ 89
3.3 Le protocole $T = 1$ 100
3.4 Les fichiers d'une carte à puce 102
3.5 Synthèse 110

4 ◦ Instructions normalisées et messages d'erreur 111
4.1 Commandes de gestion de fichiers 111
4.2 Commandes relatives à la sécurité 125
4.3 Commandes diverses 133
4.4 Signification des codes d'état SW1 et SW2 138
4.5 Les « autres » commandes 141

5 • Notions de cryptographie 143
5.1 Le vocabulaire de la cryptographie 144
5.2 Méthodes cryptographiques simples 149
5.3 Les algorithmes cryptographiques complexes à clé secrète 158
5.4 Les algorithmes cryptographiques complexes à clé publique 166

B

Applications

6 • Développement d'une application 171
6.1 Les trois familles de cartes à votre disposition 171
6.2 Lecteurs standards et lecteurs spécifiques 188
6.3 Choix d'un environnement de développement 194
6.4 Passons à la pratique 197

7 • Lecture et écriture dans une carte à puce 199
7.1 Lecteur et/ou programmateur 199
7.2 Choix et installation d'un lecteur 200
7.3 Le logiciel polyvalent CardEasy 206

8 • Personnalisation d'une carte à puce 217
8.1 Un exemple de carte personnalisable : la carte ACOS1 219
8.2 Personnalisation d'une carte avec CardEasy 228
8.3 Écriture d'une application pour carte personnalisée 235
8.4 Deux exemples d'applications pour cartes personnalisées 237

9 • Utilisation d'une carte à puce à OS ouvert 245
9.1 Le système de développement pour Basic Card 247
9.2 Une application Basic Card... sans Basic Card 250
9.3 Une clé sécurisée simple à Basic Card 260
9.4 Synthèse 269

10 ◦ Utilisation de cartes à puce spécifiques 271
10.1 Des cartes plus ou moins bien documentées 272
10.2 Lecteur/programmateur pour cartes spécifiques 282

11 ◦ Réalisez vos outils de développement et d'analyse 293
11.1 Lecteur/programmateur compatible Phoenix, SmartMouse et JDM 293
11.2 Programmateur pour cartes Fun ou Purple 305
11.3 Analyseur de dialogue universel pour cartes à puce 311

12 ◦ À la limite de la légalité 327
12.1 Les différents types d'attaques 327
12.2 Les attaques purement logicielles 328
12.3 Les attaques matérielles destructrices 329
12.4 Les attaques matérielles non destructrices 329
12.5 Les attaques externes de type SPA, DPA et EMA 330
12.6 Synthèse 337

C

Annexes

Annexe 1 ◦ Contenu du CD-Rom 341

Annexe 2 ◦ Adresses internet utiles 345

Index 347

TECHNIQUE ET INGÉNIERIE
Série EEA

GESTION INDUSTRIELLE
CONCEPTION
FROID ET GÉNIE CLIMATIQUE
MÉCANIQUE ET MATÉRIAUX
CHIMIE
ENVIRONNEMENT ET SÉCURITÉ
EEA

Christian Tavernier

LES CARTES À PUCE

Théorie et mise en œuvre

2e édition

La nouvelle édition de cet ouvrage, totalement refondue et mise à jour, présente **tous les aspects théoriques et pratiques des cartes à puce et de leurs applications**, de leur conception à leur mise en œuvre :

- **les différents types de cartes** actuelles, avec et sans contact ;
- **les jeux d'instructions**, organisation des données et messages d'erreur des cartes à puce ;
- **les diverses méthodes de cryptographie** utilisées ;
- **les environnements de développement** de tous les types de cartes à puce ainsi que leur mise en œuvre ;
- **la réalisation de lecteurs, programmateurs et outils d'investigation** dont un analyseur de dialogue universel très performant.

De nombreux exemples d'applications abondamment commentés et un CD-ROM comportant les listings source des programmes présentés, les logiciels nécessaires aux manipulations décrites, ainsi que **les versions les plus récentes des normes EMV (cartes bancaires), GSM (cartes de téléphonie mobile) et PC/SC**, complètent cet unique ouvrage de référence dans le domaine.

CONFIGURATION	MINIMALE	RECOMMANDÉE
Processeur	–	AMD Duron, Athlon, Sempron Intel Pentium IV et au-delà
Système d'exploitation	Windows 98	Windows XP
Ports de communication	Un port série RS232* Un port parallèle** Un port USB 1 ou 2***	Un port série RS232* Un port parallèle** Un port USB 2
Périphériques	Lecteur de CD ou de DVD	Lecteur de CD ou de DVD

* Nécessaire seulement si réalisation du programmateur Phoenix/JDM et/ou de l'analyseur de dialogue universel.
** Nécessaire seulement si réalisation du programmateur pour carte Fun.
*** Selon le type de lecteur de carte à puce choisi.

CHRISTIAN TAVERNIER est ingénieur conseil et professeur des universités associé en électronique, informatique et télécommunications. Spécialiste reconnu des microprocesseurs et microcontrôleurs, ses nombreux ouvrages et articles font autorité depuis plus de vingt-cinq ans.

9 782100 495115

6650634
ISBN 978-2-10-049511-5

www.dunod.com

DUNOD