



Commerce électronique

Élément de sécurité et plateforme mobile

Pierre.Paradinas@cnam.fr

P. Paradinas - 201^{OSOS}

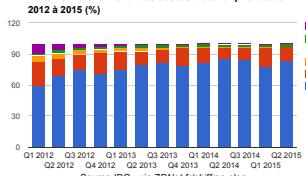


le cnam

Plateforme mobile et e-commerce

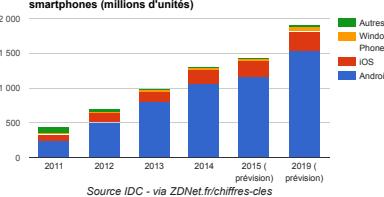
Quelques chiffres sur les accès mobiles...

Parts de marché mondiales des OS de smartphones de 2012 à 2015 (%)



Source IDC - via ZDNet.fr/chiffres-cles

Répartition par OS des livraisons mondiales de smartphones (millions d'unités)



Source IDC - via ZDNet.fr/chiffres-cles

le cnam

P. Paradinas - 201^{OSOS}

Le cours du jour

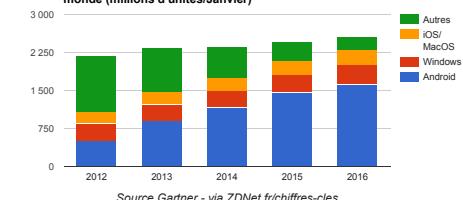
- Introduction
- Éléments de sécurité informatique et de cryptographie
- Objets sécurisés
- Java Card et protection software
- Plateforme mobile:
 - Android
 - Payment Mobile
- Sécurité des plateformes mobiles
 - TEE
 - SE

P. Paradinas - 201^{OSOS}

le cnam

Fixe/Mobile

Systèmes d'exploitation des terminaux livrés dans le monde (millions d'unités/Janvier)



Source Gartner - via ZDNet.fr/chiffres-cles
Les terminaux mobiles rebattent les cartes – Si l'y a encore des années, le PC était l'unique terminal d'accès à Internet, ce n'est assurément plus le cas désormais. Et l'explosion du nombre de terminaux mobiles a profondément modifié le rapport de force. Tous terminaux connectés confondus, la part de marché de Windows chute à 14%. L'OS dominant c'est en effet Android dont plus d'un milliard d'appareils livrés cette année devraient être équipés. Et l'OS de Google devrait encore se développer dans les toutes prochaines années.

P. Paradinas - 201^{OSOS}

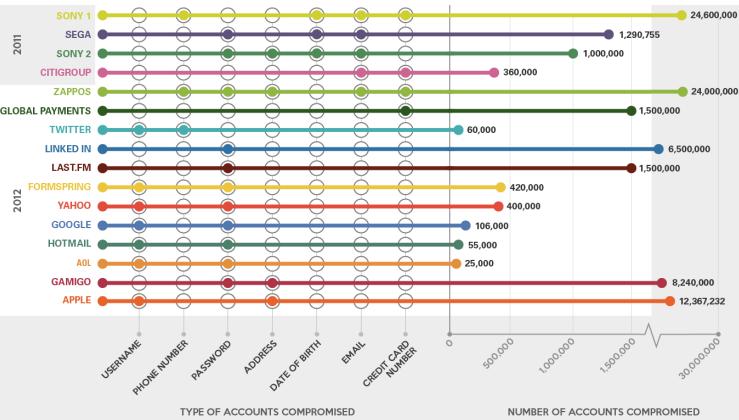
le cnam

Élément de sécurité (introduction)

P. Paradinas - 2014

le cnam

Every day there is security issue !



P. Paradinas - 2014

le cnam

...

Le groupe Target victime d'un vol géant de données bancaires

Le Monde.fr avec AFP et Reuters | 11.01.2014 à 11h19 • Mis à jour le 11.01.2014 à 12h28



Le 19 décembre, Target avait révélé que les coordonnées de 40 millions de comptes bancaires ou de cartes de crédit pourraient avoir été atteintes lors d'un "accès non autorisé" à son système informatique entre le 27 novembre et le 15 décembre. | AFP/FREDERIC J. BROWN

P. Paradinas - 2014

le cnam

ça se discute (<http://www.republique-numerique.fr/>)

Article 22 - Secret des correspondances numériques
293 votes • 17 modifications • 16 arguments • 1 source

Explication de l'article

Objectif : Renforcer le secret des correspondances privées

Explanations : Cet article est destiné à rappeler le principe du secret des correspondances privées. Conformément aux services de téléphonie ou de SMS, de nombreux services en ligne (service de téléphonie sur IP, réseaux sociaux, services de messagerie en ligne, courrier électronique etc.) analysent le contenu des messages pour commercialiser des offres. Ces pratiques doivent être encadrées pour préserver la confiance des utilisateurs dans ces services. Cet article réaffirme donc le principe essentiel du secret des correspondances en précisant l'application aux correspondances numériques. L'article précise les cas limités où des traitements automatisés peuvent analyser le contenu des correspondances (affichage, tri, acheminement, anti-spam, anti-virus).

Exemple : Certains services de correspondance privée en ligne offerts aux usagers ne pourront plus dorénavant examiner automatiquement le contenu des correspondances pour des fins commerciales.

Article 22 - Secret des correspondances numériques

L'article L. 32-3 du code des postes et des communications électroniques est ainsi modifié :

1° Au début du premier alinéa, est ajoutée la mention : « I. – »;

2° Sont ajoutés cinq alinéas ainsi rédigés :

“ II. – Les éditeurs de services de communication au public en ligne permettant aux utilisateurs de ces services d'échanger des correspondances sont tenus de respecter le secret de celles-ci. Le secret couvre le contenu de la correspondance en ligne, l'en-tête du message ainsi que les documents joints à la correspondance, le cas échéant.

“ Tout traitement automatisé d'analyse du contenu de la correspondance en ligne ou des documents joints à celle-ci constitue une atteinte au secret des correspondances, sauf lorsque ce traitement a pour fonction l'affichage, le tri ou l'acheminement de ces correspondances, ou la détection de contenus non sollicités ou malveillants.

“ L'éditeur prend les mesures nécessaires pour garantir le secret et l'intégrité des correspondances échangées par l'intermédiaire de ses services.

“ III. – Les infractions aux dispositions du présent article sont sanctionnées des peines prévues aux articles 226-1, 226-2, 226-3 et 226-15 du code pénal.

“ Les opérateurs et les éditeurs mentionnés au II sont tenus de porter à la connaissance de leur personnel les peines encourues au titre

du présent article. »

Article 26 - Définition d'un cadre de confiance pour le recommandé électronique

Article 27 - Paiement par SMS

P. Paradinas - 2014

le cnam

Et la plateforme Android...

- Article sur les plateformes Android attaquées..

ZDNet.fr - News - Télécoms - Stagefright : un simple MMS, pour contrôler 95% des smartphones Android ?

Stagefright : un simple MMS, pour contrôler 95% des smartphones Android ?

Sécurité : La vulnérabilité (corrigée) se situerait au cœur du code source d'Android Open Source Project (AOSP), selon les chercheurs de Zimperium.

ZDNet Par La rédaction de ZDNet.fr | Lundi 27 juillet 2015

Nouvelle alerte autour d'Android. Cette fois, ce sont les chercheurs de Zimperium qui ont mis la main sur une faille critique dans le code source du robot vert. La vulnérabilité est plutôt sauvage et discrète...

P. Paradinas - 201



le cnam

Computer Science Security Introduction

- Basics and definitions about confidentiality, integrity and availability
- About threats
- Policy and mechanisms
- Assumptions and trust
- Assurance
- From specifications to the program

P. Paradinas - 201



le cnam

Le problème n'est pas nouveau



P. Paradinas - 201



le cnam

Basics

- A system provides features. The **threats** may corrupt the system
- Security protects the system against threats
- Security is based on policies and mechanisms
- System security analyzing improves security
- Security is also related to trust
- Human beings are part of the system and generally the weakest link !

P. Paradinas - 201



le cnam

Basic security properties

- Confidentiality
- Integrity
- Availability

These properties are different and related to the system context

P. Paradinas - 2019 © 13

le cnam

Basic security properties: integrity

- Integrity is a feature of information where there is trust on the data (or resources) in term of alterations/modifications (data integrity) and on data origin (origin integrity some time call authentication)
- Examples:
 - In a operating system, “user management” must be based on integrity. Only “user” authorized may change the rules and authorization attached to a user
 - In a fund transfer integrity is on the amount, origin and destination
- Integrity Mechanisms:
 - Prevention (how to protect)
 - Detection (how to detect if an information was altered)

P. Paradinas - 2019 © 15

le cnam

Basic security properties: confidentiality

- Confidentiality is the feature of information where it have to be keep “secret” and not to be “revealed”
- Examples:
 - secret key involved in a cryptographic protocol
 - information “reserved” to a group of person
 - password
 - ...

P. Paradinas - 2019 © 14

le cnam

About integrity

- Integrity on check
- Integrity on payment card



P. Paradinas - 2019 © 16

le cnam

Intégrité ?

- ➊ Comme le chèque ou les billets de banque, le paiement sur Internet doit offrir de bonnes propriétés :

❖ Qui achète ?

❖ Le commerçant est-il un "vrai" commerçant ?

❖ Autre propriété : la non-réputation !



Threats/Attacks

- ➊ A **threat** is a potential violation of security. When the violation occurs, it is an **attack**. The attacks are performed by attackers
- ➋ A system must be prepared to prevent attacks and executes countermeasures
- ➌ 4 large classes of threat:
 - ❖ Disclosure (non authorized information are revealed)
 - ❖ Deception (acceptance of false data)
 - ❖ Disruption (interruption of operation)
 - ❖ Usurpation (non authorized control of the system)

Basic security properties: availability

- ➊ Availability refers to the possibility to use data or resources of a system
- ➋ Availability is part of the security issues as if some one establish conditions where the data or resources of a system are no longer available for a normal use it causes a "deny of access"
- ➌ Examples:
 - ❖ DOS on Internet are well known
 - ❖ If a bank network is not available the day before Christmas then many commercial transactions will be impossible or done without "confirmation" from the bank
- ➍ The system design (statical, expected pattern, parameters,...) defines a usage model, if it fails we enter in DOS
- ➎ DOS detection is very complex task

Different threats

- ➊ Snooping (wiretapping, passive wiretapping)
- ➋ Modification
- ➌ Masquerade
- ➍ Delegation
- ➎ Repudiation of origin
- ➏ Denial of receipt
- ➐ DOS

Policy and mechanism

- ➊ Definition: A security policy is a statement of what is, and what is not allowed
 - ✖ A security policy specifies “secure” and “non secure” states and actions
- ➋ Definition: A security mechanism is a method, tool, or procedure for enforcing a security policy
- ➌ A security policy can (must) be defined by mathematical and formal technics
- ➍ Example:
 - ✖ Change its password is allowed for an entity
 - ✖ Request a proof of an identity before to accept to change a password is a security mechanism

P. Paradinas - 201^{POSSO} 21

le cnam

Goals of policy and mechanism

- ➊ For a given security policy security mechanisms can:
 - ✖ Prevent
 - ➏ In this case attacks fail, attacks are not efficient,
 - ✖ Detect
 - ➏ The mechanism is able to detect that attacks are performed, detected and have to be reported
 - ✖ Recovery
 - ➏ Is the set of actions necessary to put in place to reach and establish a new “secure state” of the system

P. Paradinas - 201^{POSSO} 22

le cnam

Assumptions and Trust

- ➊ In real word, mechanisms are broad
- ➋ Trust in mechanisms requires assumptions:
 - ✖ Each mechanism implement one or more part of the security policy
 - ✖ The union of mechanisms implements the all policy
 - ✖ The mechanism are correctly implemented, installed and managed during the life cycle of the system

P. Paradinas - 201^{POSSO} 23

le cnam

Assurance

- ➊ Trust is difficult to evaluate ? How much you trust a system ?
- ➋ How you develop your system provides an assurance level of the trust in the system
- ➌ A system is said to **satisfy** a specification if the specification correctly states how the system will function

P. Paradinas - 201^{POSSO} 24

le cnam

Specification

- Specifications are a precise statement of the system behaviors
 - ✿ It describe what the system is allow to do (and not to do)
- The specification may be formal (based on mathematical or formal language) or informal (set of phrases) description
- The level of description may be different (low or high level language description)
- The specification are not only relevant to security function but on the system itself
 - ✿ Use the same formalism is challenging and benefit for the system
- Security is a non functional property

P. Paradinas - 201^{POSSO} 25

le cnam

Design and implementation

- The **design** of a system transforms the specification into a component that will implement them
 - ✿ The design is said to satisfy the specifications, in any cases, the design will not permit the system to violate the specification
- The design **implementation** realizes the functions (execute the "system functions")
 - ✿ On CS it is a program executable on an engine
 - ✿ By transitivity an implementation satisfy a system specification
 - ✿ A **program** is correct if its implementation performs as specified
 - Proof of program is very complex and difficult to do !
 - ✿ As correctness is a big issue, a posteriori techniques like verification of the system by **testing** are performed

P. Paradinas - 201^{POSSO} 26

le cnam

Operational issues and others points

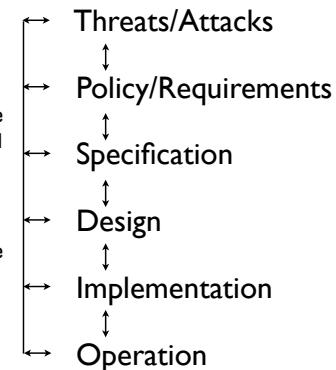
- Cost benefit analysis
- Risk analysis
- Laws and customs (cryptography)
- Certifications
- Organizational problems
- People problems
 - ✿ inside and outside

P. Paradinas - 201^{POSSO} 27

le cnam

Not so simple

- The different notions are "interleaved" and nested
- System is in "real world" and the word changes !
- The cost of security have to be compared with the system (and threats) costs



P. Paradinas - 201^{POSSO} 28

le cnam

Élément de cryptographie

P. Paradinas - 2019  29

le cnam

Éléments de cryptographie (Alice et Bob)



Alice and Bob cartoon by John Richardson in Physics World, March 1998

http://en.wikipedia.org/wiki/Alice_and_Bob

P. Paradinas - 2019  30

le cnam

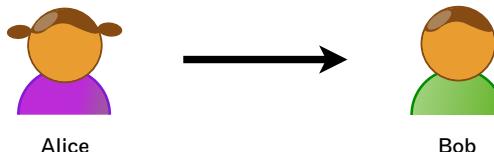
Pourquoi

- ➊ Pourquoi échanger des informations secrètement (secrètes) ?
- ➋ Les informations :
 - 🔊 Militaires
 - 🔊 Economiques et le commerce électronique
 - 🔊 Personnelles
- ➌ On se protège contre quoi ?

P. Paradinas - 2019  31

le cnam

Protéger de...

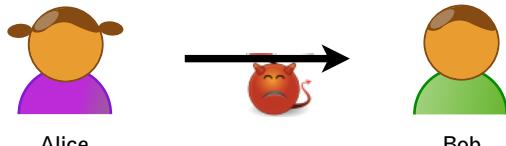


- ➌ Quelles propriétés/caractéristiques

P. Paradinas - 2019  32

le cnam

Protéger de quoi de qui,...



- Confidentialité
- Intégrité
- Authenticité

P. Paradinas - 2010 [33]

le cnam

Comment : exemple (simple à ne pas suivre)

Substitution

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Message : "bienvenue au musée du cnam"

Message chiffré :

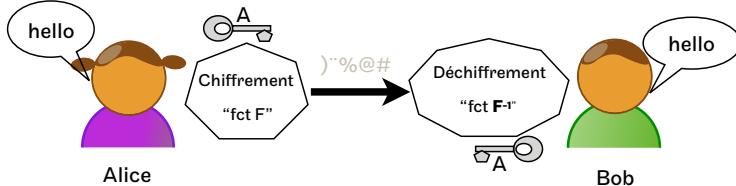
UXGOXGNX....

à vous de continuer

P. Paradinas - 2010 [34]

le cnam

Un peu de formalisme



P. Paradinas - 2010 [35]

le cnam

Vers un système parfait

Intuitivement

La clé est une chaîne infinie aléatoire...

Le texte est composé avec la clé...

Le texte chiffré....

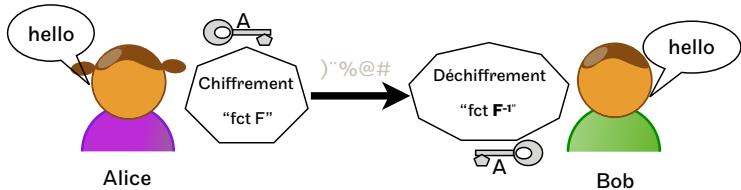
La clé est une chaîne infinie aléatoire...

Le texte est composé avec la clé...

P. Paradinas - 2010 [36]

le cnam

Algorithme symétrique



- Chiffrement
- Signature ?
- Distribution des clés ?

P. Paradinas - 2010

le cnam

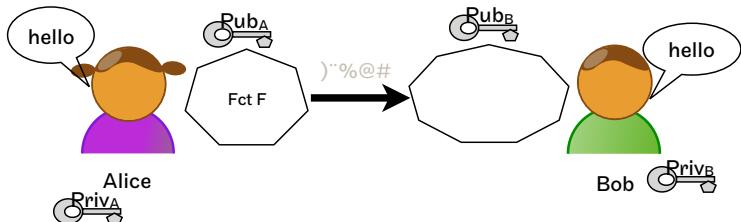
Algorithme symétrique : exemple

- 1970-2000 :
 - ✿ DES (Data Encryption Standard) proposé par le NIST (FIPS 46-2), en 1977
 - ✿ Recherche exhaustive sur la clé de 56 bits => 2^{56} "attaques réalisable" => utilisation du Triple-DES
- 2000-2004
 - ✿ AES (Advanced Encryption Standard) standard NIST : FIPS 197
 - ✿ Taille de bloc de 128 bits
 - ✿ Tailles de clé de 128, 192 et 256 bits

P. Paradinas - 2010

le cnam

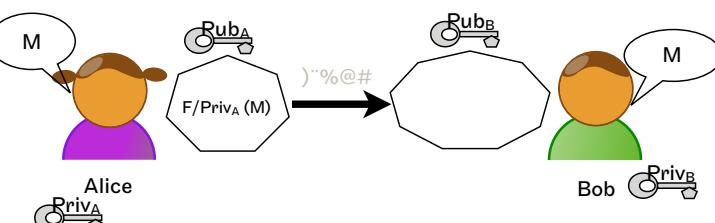
Algorithme asymétrique



P. Paradinas - 2010

le cnam

Algorithme asymétrique (signer)

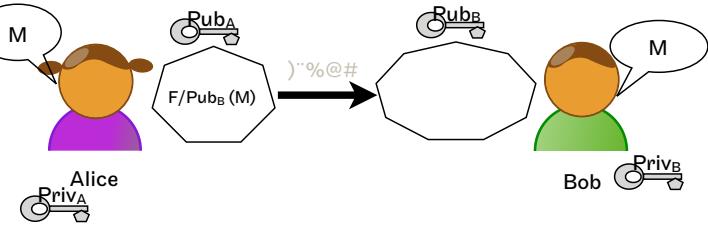


- Signer un message M
- Alice envoie : $F/\text{Priva}_A(M)$ à Bob
- Bob vérifie : $F^{-1}/\text{Pub}_A[F/\text{Priva}_A(M)]$

P. Paradinas - 2010

le cnam

Algorithme asymétrique (chiffrer)



- ➊ Chiffrer un message M
- ➋ Alice envoie : $F/\text{Pub}_B(M)$ à Bob
- ➌ Bob déchiffre le : $F^{-1}/\text{Priv}_B[F/\text{Pub}_B(M)]$

P. Paradinas - 2014

le cnam

Sécurité du RSA

- ➊ Attaque par la force brute => retrouver p & q en connaissant n
- ➋ La sécurité de l'algorithme RSA repose sur deux conjectures :
 - ⌚ « casser » RSA implique de factoriser n ($n = p * q$)
 - ⌚ le temps que prend cette factorisation est exponentiellement avec la longueur de la clé
- ➌ On arrive à factoriser des grands nombres de 768 bits (2009)
- ➍ Prendre des clés 2048 voir même 4096...

P. Paradinas - 2014

le cnam

Exemple d'algorithme : RSA

- ➊ Le concept de cryptographie asymétrique : Whitfield Diffie et à Martin Hellman avec une publication en 1976 (New Directions in Cryptography)
- ➋ 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman du MIT donne
 - ➌ Choisir p et q, deux nombres premiers distincts ;
 - ➍ Module de chiffrement : $n = pq$;
 - ➎ $\varphi(n) = (p - 1)(q - 1)$;
 - ➏ e premier avec $\varphi(n)$ appelé exposant de chiffrement ;
 - ➐ d, inverse de e modulo $\varphi(n)$, exposant de déchiffrement.
- ➑ Chiffrement : $C = M^e \pmod{n}$
- ➒ Déchiffrement : $M = C^d \pmod{n}$

P. Paradinas - 2014

le cnam

Protocole (TLS/SSL)

- ➊ Les algorithmes sont utilisés dans des protocoles : identification, authentification,...
- ➋ Dans le monde du Web TLS/SSL est très utilisé
 - ⌚ Transport Layer Security (TLS), et son précurseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet
 - ⌚ SSL a été introduit par Netscape puis repris par IETF
 - ⌚ Objectifs de TLS :
 - ➌ l'authentification du serveur ;
 - ➍ la confidentialité des données échangées ;
 - ➎ l'intégrité des données échangées ;
 - ➏ l'authentification du client (option).
 - TLS v1.0 en 1999, TLS v1.1 en 2006 et TLS v1.2 en 2008, v1.3 en cours de discussion

P. Paradinas - 2014

le cnam

Mise en œuvre

- ➊ Depuis les années 2005-2010, déploiement large
- ➋ Pour l'utilisateur :
 - ➌ Dans les navigateurs Web :
 - ➍ l'URL dans la barre d'adresse commence par **https**
 - ➎ signe distinctif sur le navigateur (cadenas)
 - ➏ le passage en jaune de la barre d'adresse (cas de Firefox).

P. Paradinas - 2010 © 45

le cnam

Principe (1/3)

- ➌ (2) si aucun certificat ne fonctionne, le navigateur web utilise la clé publique envoyée par le serveur :
 - ➍ Si OK, i.e. : le serveur Web a son certificat => message d'avertissement (serveur potentiellement frauduleux)
 - ➎ Si NotOK, le certificat est invalide => la connexion échoue !
- ➍ Client : le navigateur génère une clé de chiffrement symétrique, ce sera la appelée clé de session. La clé de session est envoyée chiffré au serveur
 - ➎ Sans authentification du client : la clé de session est avec la clé publique du serveur
 - ➏ Option : *le client chiffre la clé de session avec sa propre clé privée et envoie son certificat au serveur.*

P. Paradinas - 2010 © 47

le cnam

Principe (1/3)

- ➊ Client : demande de connexion sécurisée
- ➋ Serveur :
 - ➌ envoie son certificat, contenant la clé publique, des informations d'identification et une signature chiffrée
 - ➍ optionnel : *demande une demande d'authentification du client*
- ➌ Client:
 - ➍ (1) déchiffre la signature chiffrée en utilisant les certificats des autorités de certifications (AC) [intégrés par défaut dans le navigateur]
 - ➎ vérification auprès de l'AC que le certificat est valide (date, révocation)

P. Paradinas - 2010 © 46

le cnam

Principe (3/3)

- ➌ Serveur :
 - ➍ déchiffre la clé de session envoyée par le client :
 - ➎ avec sa clé privée (pas d'authentification du client)
 - ➏ ou avec la clé publique envoyée par le client
 - ➎ Les échanges sont faits avec la clé de session partagée par le client et le serveur
 - ➏ La connexion TLS est établie.
 - ➐ ...
 - ➑ Le serveur révoquera la clé de session après déconnexion de l'utilisateur ou une durée d'inactivité déterminée

P. Paradinas - 2010 © 48

le cnam

Objets sécurisés

P. Paradinas - 2017 © 49

le cnam

JAVA CARD

P. Paradinas - 2017 © 50

le cnam

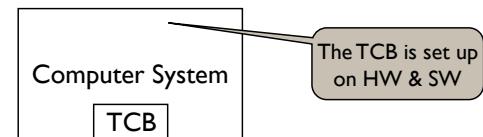
Trust-OS

P. Paradinas - 2017 © 51

le cnam

Trusted computing base (TCB)

- Initial definition came from classical security paper of B. Lampson, M. Abadi, M. Burrows and E. Wobber, *Authentication in Distributed Systems: Theory and Practice*, ACM Transactions on Computer Systems (1992).
- TCB definition of a computer system is: *a small amount of software and hardware that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security.*



P. Paradinas - 2017- © 52

le cnam

An other definition (evaluation approach)

- ➊ From Orange book (Trusted Computer System Evaluation Criteria, a computer security standard)
 - ✖ Available until 2002 under the number of (DoD 5200.28-STD)
 - ✖ A formal definition of the TCB of a computer system, as
 - ➊ “the totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy”.
 - ✖ and explain later
 - ➊ “the ability of a trusted computing base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy”.

P. Paradinas - 2017- 

le cnam

How to develop a TCB

- ➋ Prove a complete software is a huge challenge
- ➋ There is no many example of software develop with automatic proved system in OS environment
 - ✖ 1st “important” proposition seL4 is an example of complete proof of OS microkernel
 - ➊ Performed by NICTA (Australia)
 - ➊ A large team (13 authors)
 - 8 700 C-LOC and 600 Assembler-LOC
 - 200 000 Isabelle-“LO script”
 - Initial dev : Code 8 py and Proof 20 py, next version will be less and around 8 py
 - ➋ Publication in SOSP 2009
 - seL4: Formal Verification of an OS Kernel

P. Paradinas - 2017- 

le cnam

OS approach

- ➊ A. Tanenbaum in Modern Operating Systems book introduces the trusted computing base (TCB).
 - ✖ “At the heart of every trusted system is a minimal TCB consisting of the hardware and software necessary for enforcing all the security rules.”
 - ✖ “In a secure design, often the TCB will be quite separate from the rest of the operating system in order to minimize its size and verify its correctness.”

P. Paradinas - 2017- 

le cnam

New and others propositions

- ➊ Sysgo and the european project EUROMILS
 - ✖ EURO-MILS: Secure European virtualisation for trustworthy applications in critical domains
- ➋ The EC project Euromils : <http://www.euromils.eu>
 - ➊ Focus onMILS (Multiple Independent Levels of Security), with high-assurance security architecture that supports the coexistence of untrusted and trusted components, based on separation mechanisms and controlled information flow
 - ➋ Trustworthiness by design is achieved by virtualisation, allowing us to combine heterogeneous domains (e.g. applications of different trustworthiness, different networks) and to set up trustworthy communication
 - ➌ A methodology based on the “Common Criteria” security standard to its highest levels of assurance, including formal verification engineering

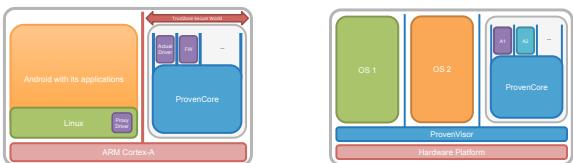
➌ <http://www.euromils.eu>

P. Paradinas - 2017- 

le cnam

New and others propositions (cont'd)

- Prove & Run proposition is based on ProvenCore a proven Micro Kernel and/or ProvenHypervisor :



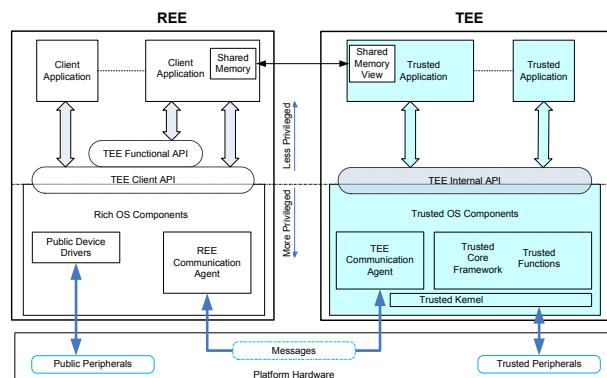
- <http://www.provenrun.com/wp-content/uploads/2016/02/Proven-Security-for-the-Internet-of-Things-v2.pdf>

P. Paradinas - 2017- CC BY-NC-SA

le cnam

More detail on architecture

Figure 3-1: TEE System Architecture



P. Paradinas - 2017- CC BY-NC-SA

le cnam

TEE: Trusted Execution Environment

- This specification defines a communications API for connecting Client Applications running in a rich operating environment with security related Trusted Applications running inside a Trusted Execution Environment (TEE).

- a TEE is expected to be a trusted environment within the main device system-on-a-chip, which complements traditional security environments such as a UICC SIM card, although this is not a requirement of the API.

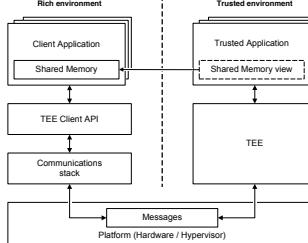


Figure 2-1: TEE Client API System Architecture

P. Paradinas - 2017- CC BY-NC-SA

le cnam

TEE (cont'd)

- A TEE provides an execution environment with security capabilities, which are either available to Trusted Applications running inside the TEE or exposed externally to Client Applications.
- See the Open Mobile Trusted Platform (OMTP) Advanced Trusted Environment for a requirements analysis of Trusted Execution Environments in mobile devices.



P. Paradinas - 2017- CC BY-NC-SA

le cnam

New and others propositions (cont'd)

- CertikOS : Usenix 2016

P. Paradinas - 2017- 

le cnam

Formal proof and code

- In the work of NICTA on seL4 a part of the work is done by human translation...
 - ✖ subject to errors, mistake, misunderstanding
- How to get a complete automatic proof ?

P. Paradinas - 2017- 

le cnam

TCB and certification

- TCB needs to be small. The assurance process is very expensive
 - ✖ Effort in term of code review
 - ✖ Effort in certification
 - Many PP on Operating System : essentially on the separation
 - 2PP
 - COTS Compartmentalized Operations Protection Profile Operating Systems : EAL4 (.uk)
 - Operating System Protection Profile, Version 2.0 EAL 4+ (.de)
 - 96 Products on 1750
 - Example EAL 6+ : Green Hills Software INTEGRITY-178B Separation Kernel, comprising: INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0402-GH01_Rel (Version 4.2) running on Compact PCI card, version CPN 944-2021-021 w/PowerPC, version 750CXE

P. Paradinas - 2017- 

le cnam

TCB size and OS debate

- Effort in proof of code with formal method
- This point is discussed in a paper between A. Tannenbaum and L. Torvald about microkernel and monolithic kernel[in 1992, news&users groups]

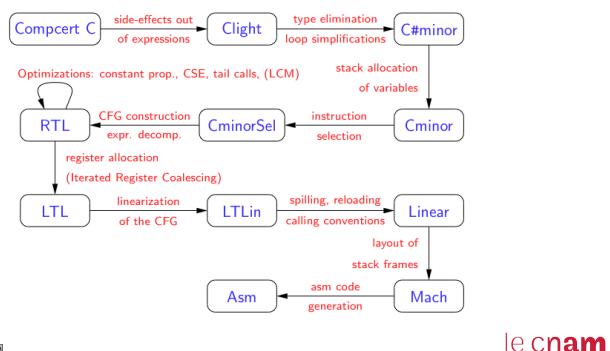
P. Paradinas - 2017- 

le cnam

CompCert

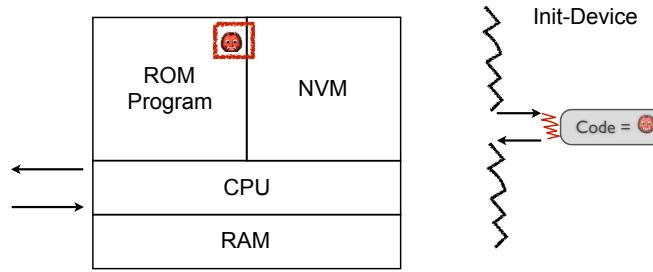
- Few words about CompCert a project of Xavier Leroy @INRIA
Gallium team and cooperation with persons from CNAM/CEDRIC

• <http://compcert.inria.fr>



TCB and others problems

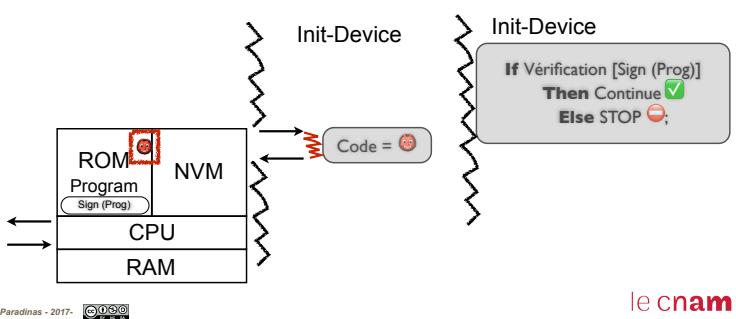
- Trust with the right program and data ?



le cnam

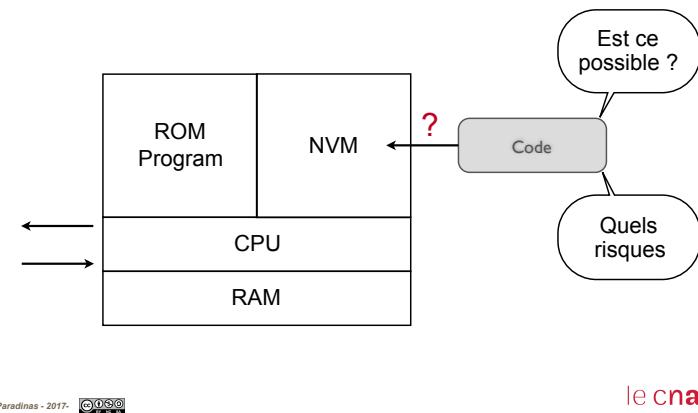
Trusted Boot

- During initialisation and boot, verification of software integrity is necessary
- The verification needs to be done in the fabrication and deployment process (Who ? When ? Where ? How ?)



Exercice

- Ajouter du "code" dans un environnement microcontrôleur :



Plateforme mobile

- Plateforme matérielle et réseau GSM
- Plateforme logicielle

P. Paradinas - 2010 69

le cnam

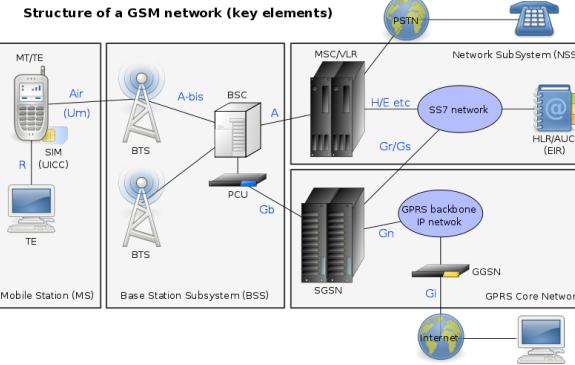
Plateforme mobile

- Plateforme matérielle et réseau GSM
- Plateforme logicielle (Android)

P. Paradinas - 2010 71

le cnam

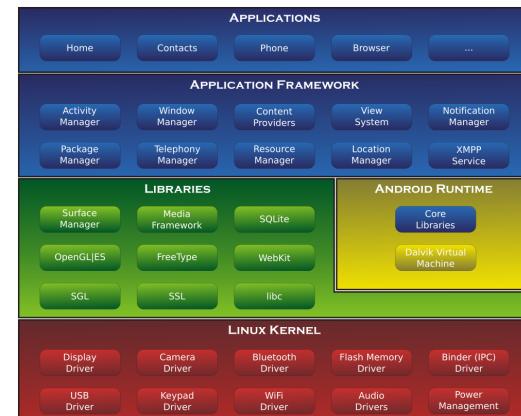
Sur le réseau de téléphonie mobile



P. Paradinas - 2010 70

le cnam

Android : architecture générale



P. Paradinas - 2010 72

le cnam

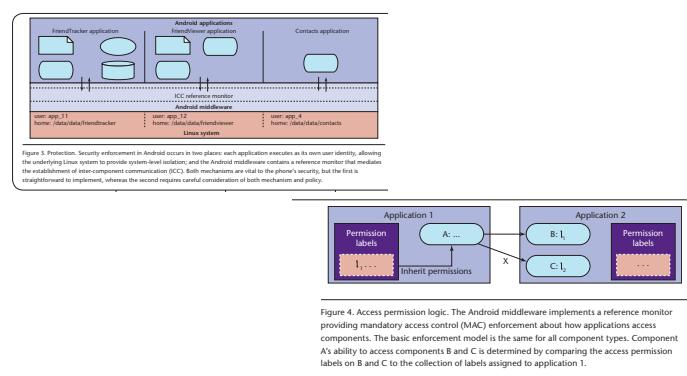
Android, noyau Linux et services

- ➊ Le noyau Linux est utilisé pour les fondations d'Android;
 - ➋ i.e. : les services classiques des systèmes d'exploitation :
 - ➌ utilisation des périphériques,
 - ➌ accès aux réseaux de télécommunication,
 - ➌ manipulation de la mémoire et des processus et
 - ➌ le **contrôle d'accès**.
- ➊ Services pour l'exploitation des réseaux de télécommunications GSM, Bluetooth, Wi-Fi et UMTS, et l'envoi de messages SMS

P. Paradinas - 2010 [OSO] 73

le cnam

Sécurité dans Android



P. Paradinas - 2010 [OSO] 75

le cnam

Android et Java

- ➊ Android comporte une machine virtuelle nommée Dalvik, différente de la JVM elle a été conçue pour les appareils mobiles et leurs ressources réduites
- ➊ Le bytecode de Dalvik est différent de celui de la machine virtuelle Java de Oracle (JVM):
 - ➋ compilation standard en bytecode pour JVM
 - ➋ puis traduction en bytecode pour Dalvik par un programme inclus dans Android
- ➌ les grandes différences sont dans les bibliothèques d'interface graphique AWT et Swing

P. Paradinas - 2010 [OSO] 74

le cnam

Développement d'application

- ➊ Le développement d'applications pour Android utilise un plug in Eclipse:
 - ➋ le JDK de la plate-forme Java,
 - ➋ des outils pour Android :
 - ➌ pour manipuler le téléphone ou la tablette, de la simuler, de créer des fichiers APK (les fichiers de paquet d'Android), débug et **signature** de l'application développée.

P. Paradinas - 2010 [OSO] 76

le cnam

Android et son environnement

- Android est aussi un environnement de développement :
 - un émulateur de téléphone ;
 - un plugin Eclipse peut aussi être considéré comme une fonctionnalité d'Android.
- Google Play : une boutique en ligne permettant l'achat et le téléchargement d'applications pour Android.



P. Paradinas - 2015 77

le cnam



Google déploiement

- Répartition des différentes versions sur le Google Play Store, au 5 octobre 2015

Version	Nom de code	Date de sortie	Version API	%
2.2	Froyo	20 mai 2010	8	0,2 %
2.3.3 - 2.3.7	Gingerbread	6 décembre 2010	10	3,8 %
4.0.3 - 4.0.4	Ice Cream Sandwich	19 octobre 2011	15	3,4 %
4.1.x	Jelly Bean	9 juillet 2012	16	11,4 %
4.2.x	Jelly Bean	13 novembre 2012	17	14,5 %
4.3	Jelly Bean	24 juillet 2013	18	4,3 %
4.4	KitKat	31 octobre 2013	19	38,9 %
5.0	Lollipop	3 novembre 2014	21	15,9 %
5.1	Lollipop	9 mars 2015	22	7,9 %

P. Paradinas - 2015 78

le cnam

Android et le libre

- But de l'OHA :
 - "favoriser l'innovation sur les appareils mobiles en fournissant une plate-forme véritablement ouverte et complète"
- est gratuit
- Android est distribué en open source sous licence Apache. La licence autorise les constructeurs qui intègrent Android dans leurs appareils à y apporter des modifications leur permettant de se distinguer de leurs concurrents et il a été adopté par de nombreux constructeurs de produits concurrents de l'iPhone.
- Libre mais... code souvent abscons...

P. Paradinas - 2015 79

le cnam



Android et sécurité

- Lors de l'été 2015, Android doit faire face à plusieurs crises. La première concerne la faille Stagefright. Elaborée par un chercheur en sécurité, elle peut perturber 95% des terminaux fonctionnant avec l'OS de Google par un simple MMS. Le pirate peut ainsi avoir accès à quasiment toutes les données sur le téléphone¹⁴. La deuxième est un bug découvert par des chercheurs Trend Micro qui paralyse téléphones et tablettes¹⁵.

P. Paradinas - 2015 80

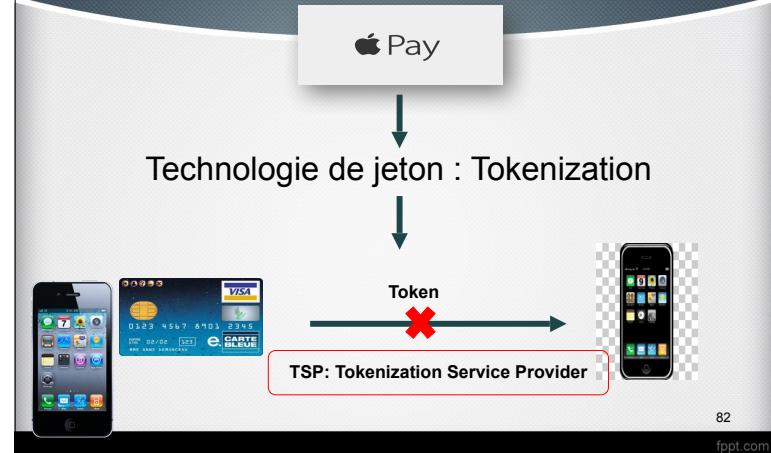
le cnam

Apple Pay

P. Paradinas - 2014 81

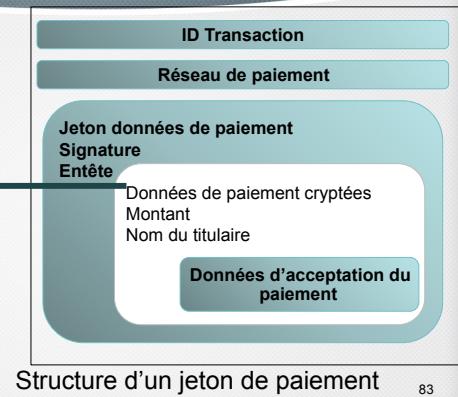
le cnam

Principe de fonctionnement Apple Pay

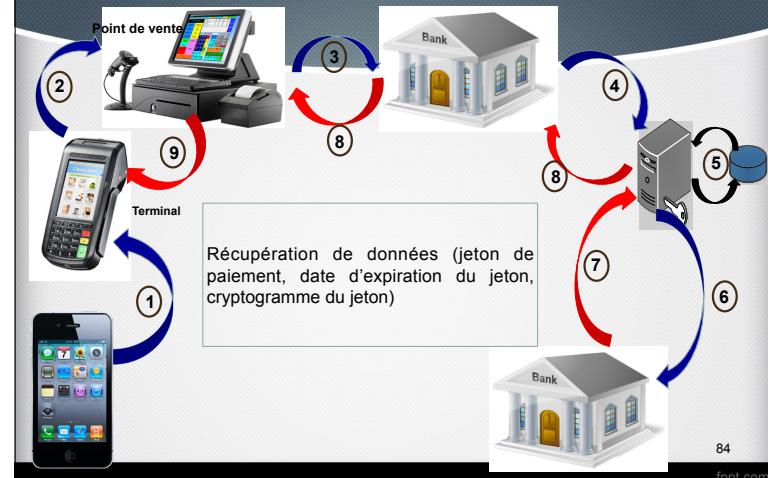


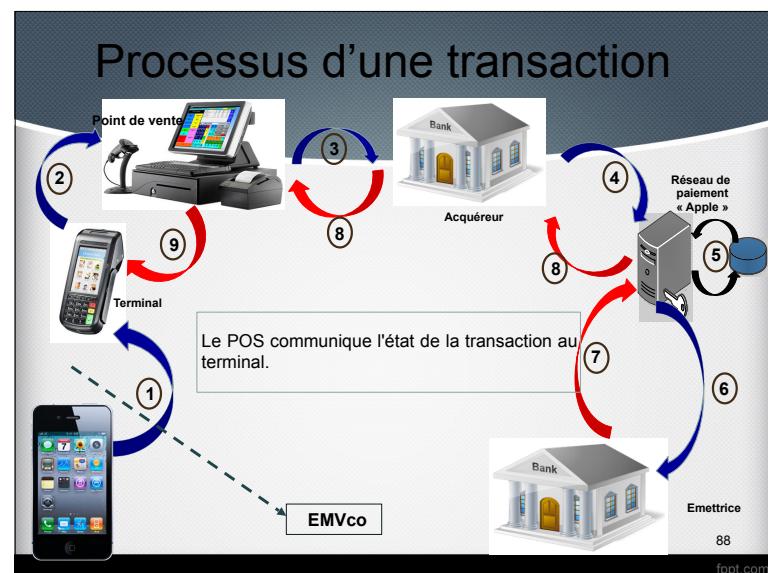
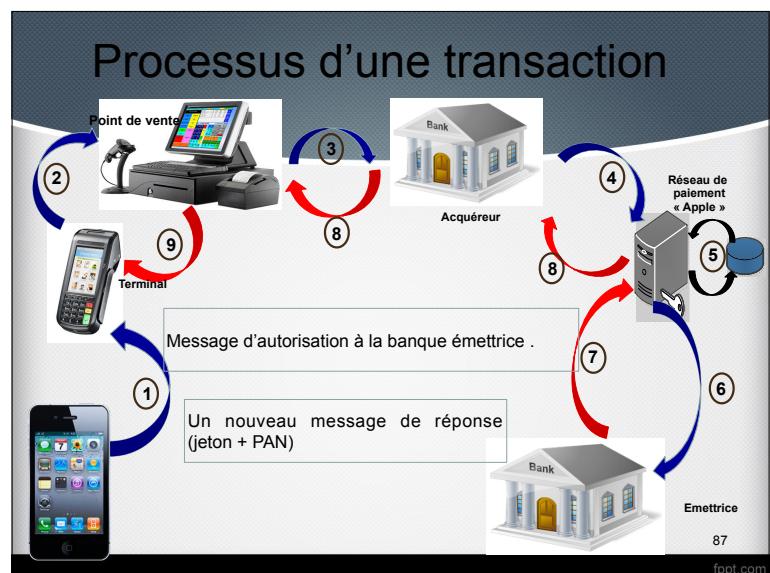
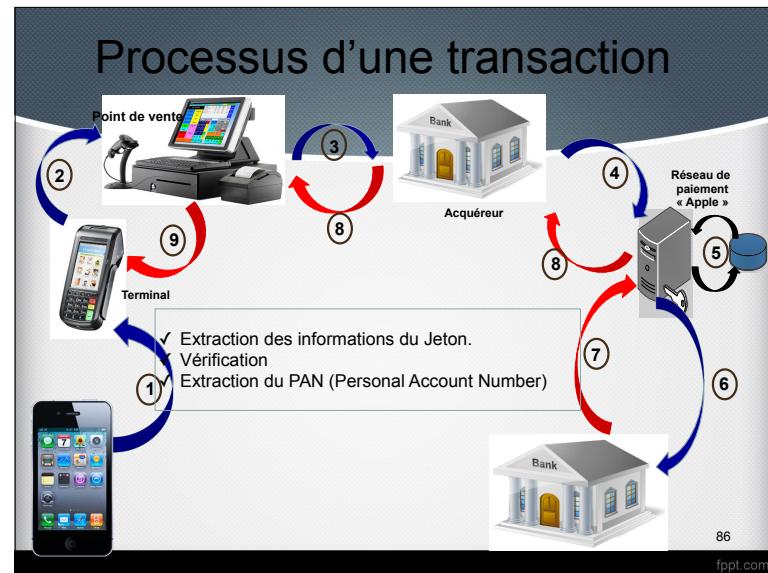
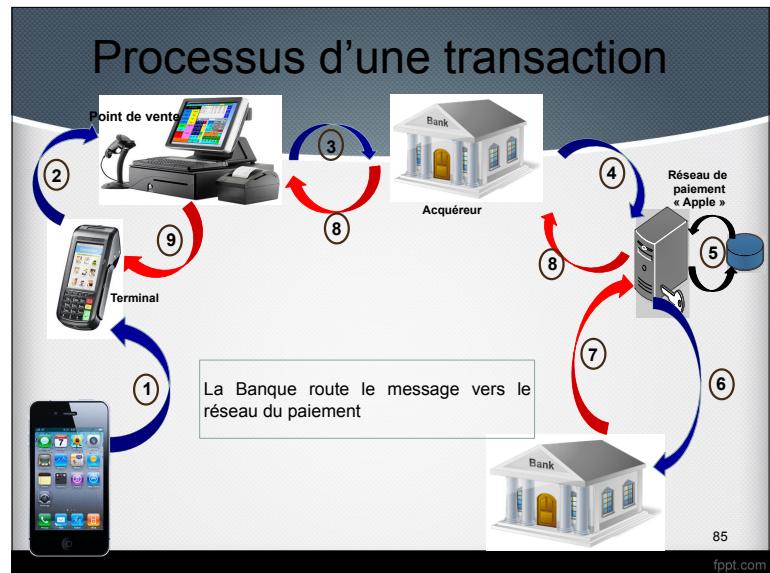
Technologie Segmentation (Tokenization)

le numéro de la carte bancaire, date d'expiration, nom, prénom → chiffré et stocké dans le SE



Processus d'une transaction





Le protocole

- ➊ Le client sélectionne la carte qu'ils veulent utiliser pour la transaction.
- ➋ Terminal sélectionne la "carte" et récupère les données nécessaires à la transaction (de jeton de paiement, jeton date d'expiration, cryptogramme jeton)
- ➌ Le point de vente (POS) communique avec le terminal de paiement et récupère les résultats de l'opération. Ceci est analysé dans le message (1100) de la demande d'autorisation ISO-8583.
- ➍ La banque acquiseuse route le message vers le réseau de paiement (réseau Apple).
- ➎ Le réseau de paiement décode le message et extrait les informations du jeton. Le cryptogramme et la date d'expiration jeton sont vérifiés et s'ils sont corrects, alors le PAN (Primary Account Number) du client est extrait de la base de données du jeton.
- ➏ Message d'autorisation à la banque émettrice
- ➐ La banque émettrice renvoie alors un message de réponse d'autorisation (1110) au réseau de paiement.
- ➑ Le réseau de paiement construit jeton à partir du PAN contenue dans le message de réponse, et met en forme un nouveau message de réponse. Ensuite, ce nouveau message est passé à travers le réseau de la banque acquiseuse vers le POS.
- ➒ Le POS communique l'état de la transaction au terminal.

P. Paradinas - 201  89

le cnam

Apple Pay/Google pay

- ➊ Apple Pay utilise un SE (Secures Elements) :

➎ élément physique dans lequel des informations confidentielles sont stockées (numéro de compte, mot de passe, ...) et qui dispose d'un capacité de calcul (chiffrement/déchiffrement/signature)

- ➋ Google Wallet utilise une technologie logicielle : Host card emulation (HCE) :

➏ en lien avec le contrôleur NFC du téléphone qui redirige la communication entre le terminal et le système d'exploitation Android

P. Paradinas - 201  90

le cnam

Google Wallet

Apple pay

Il peut fonctionner en arrière-plan sans que l'utilisateur ne voie rien.	Le numéro de la carte bancaire enregistré dans le SE.
La sécurisation de la transaction se fait dans le cloud de Google.	Génération d'un identifiant unique (comme le code de vérification au dos de la carte de crédit) CVV.
Indépendante des fabricants de smartphone et de carte SIM ainsi que des opérateurs Telecom.	Identification par empreinte digitale.
Les normes de sécurité sont encore en cours de définition.	Système de jetons, Le jeton est envoyé vers le terminal du commerçant ne peut être déchiffré afin d'obtenir le numéro de la carte de crédit En cas de vol l'utilisateur pourra désactiver le "device account number" depuis son compte Apple, le rendant inutilisable.
Code PIN peut être demandé pour les petites sommes (les sommes inférieures à 20 euro).	
Pas de solution universelle entre OS.	la puce NFC de l'iPhone 6 ou de l'Apple Watch n'est pas (comme celle des puces des cartes bancaires sans contact), activée en permanence

P. Paradinas - 201  91

le cnam

SE : Security element

- ➊ Infineon :

Embedded Secure Elements - IC [®]				
SLE 97CNF8004PE Optimized 500kByte FLASH™	SLE 97CSNF8004PE Optimized 500kByte FLASH™	SLE 97CNFX1M04PE Optimized 500kByte FLASH™	SLE 97CSNF1X1M04PE Optimized 500kByte FLASH™	SLE 97CNFX1M34PE Optimized 500kByte FLASH™
32-bit SWP Security Cryptoccontroller designed for Embedded Secure Element	32-bit SWP Security Cryptoccontroller designed for Embedded Secure Element	32-bit SWP Security Cryptoccontroller designed for Embedded Secure Element	32-bit SWP Security Cryptoccontroller designed for Embedded Secure Element	32-bit SWP Security Cryptoccontroller designed for Embedded Secure Element
ISO 7816, SWP (Mifare compatible) CPU 80MHz, 1.3MB Flash, 32kB RAM 800kByte SOLID FLASH™, 32kB RAM	ISO 7816, SWP (Mifare compatible) CPU 80MHz, 1.3MB Flash, 32kB RAM 800kByte SOLID FLASH™, 32kB RAM	ISO 7816, SWP (Mifare compatible) CPU 80MHz, 1.3MB Flash, 32kB RAM 1MBByte SOLID FLASH™, 32kB RAM	ISO 7816, SWP (Mifare compatible) CPU 80MHz, 1.3MB Flash, 32kB RAM 1MBByte SOLID FLASH™, 32kB RAM	ISO 7816, SWP (Mifare compatible) CPU 80MHz, 1.3MB Flash, 32kB RAM 1.3MBByte SOLID FLASH™, 32kB RAM
32-bit	32-bit	32-bit	32-bit	32-bit
3DES, AES up to 256-bit RSA up to 4096-bit, ECC up to 521-bit -25 to +85°C	3DES, AES up to 256-bit RSA up to 4096-bit, ECC up to 521-bit -25 to +85°C	3DES, AES up to 256-bit RSA up to 4096-bit, ECC up to 521-bit -25 to +85°C	3DES, AES up to 256-bit RSA up to 4096-bit, ECC up to 521-bit -25 to +85°C	3DES, AES up to 256-bit RSA up to 2048-bit, ECC up to 521-bit -25 to +85°C
SMD, Chip Scale Package, Wafer Sawn	SMD, Chip Scale Package, Wafer Sawn	SMD, Chip Scale Package, Wafer Sawn	SMD, Chip Scale Package, Wafer Sawn	Chip Scale Package, Wafer Sawn
Embedded Secure Element, Mobile Payment	Embedded Secure Element, Mobile Payment	Embedded Secure Element, Mobile Payment	Embedded Secure Element, Mobile Payment	Embedded Secure Element, Mobile Payment
CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo

P. Paradinas - 201  92

le cnam

Sécurité et plateforme mobile

P. Paradinas - 201^{©cnam} 93

le cnam

Mobile phone security

- What it is important to protect ?
 - ❖ Data (calendar, contact, access code...)
 - ❖ Identity of the phone owner
 - ❖ Availability
- What are the threats
 - ❖ Professional, thieves and hackers
- Who are the attacker (same as IT)
 - ❖ ...
- Consequences
 - ❖ ...

P. Paradinas - 201^{©cnam}

94

Mobile phone security

- Consequences
 - ❖ Data deletion, loss, stolen,...
 - ❖ Record conversations between the users
 - ❖ Decrease HS performances (battery)
 - ❖ Phone calls perform on number taxed
 - ❖ Use as a zombie machine
 - ❖ ...

P. Paradinas - 201^{©cnam}

95

What are the technics

- Attacks on:
 - ❖ Attack based on SMS & MMS
 - ❖ Attacks based on communication networks
 - GSM
 - Wi-Fi, Bluetooth
 - ❖ Physical attacks and reverse engineering

P. Paradinas - 201^{©cnam}

96

What are the technics (cont'd)

- Attacks based on vulnerabilities in software
 - ✖ OS
 - ✖ Web and App
 - ✖ Malicious Software (Malware)
 - ✖ Viruses and Trojans
 - ✖ Spyware
 - Long list on the wikipedia article

P. Paradinas - 201 

97

Contermeasure

- Hardware
- Firmware, bootloader
- Operating System
 - ✖ With isolation, rights,...
 - ✖ Memory protection and sand box mechanisms
 - ✖ Applications distribution model
- But also...

P. Paradinas - 201 

98

TEE: Trusted Execution Environement

- This specification defines a

communications API for connecting Client Applications running in a rich operating environment with security related Trusted Applications running inside a Trusted Execution Environment (TEE).

✖ a TEE is expected to be a trusted environment within the main device system-on-a-chip, which complements traditional security environments such as a UICC SIM card, although this is not a requirement of the API.

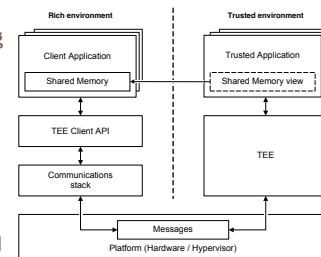


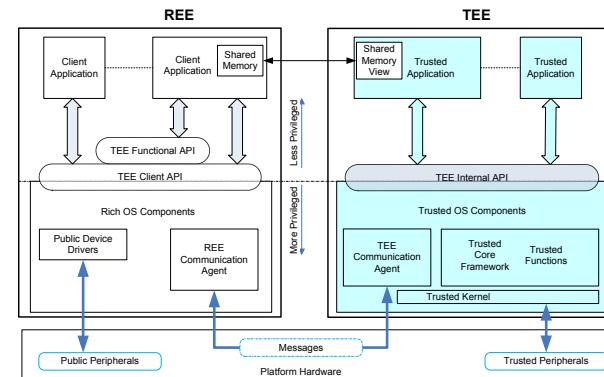
Figure 2-1: TEE Client API System Architecture

P. Paradinas - 201 

99

More detail on architecture

Figure 3-1: TEE System Architecture



P. Paradinas - 201 

100

TEE (cont'd)

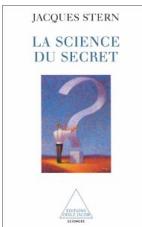


- ➊ A TEE provides an execution environment with security capabilities, which are either available to Trusted Applications running inside the TEE or exposed externally to Client Applications.
- ➋ See the Open Mobile Trusted Platform (OMTP) Advanced Trusted Environment for a requirements analysis of Trusted Execution Environments in mobile devices.

P. Paradinas - 201

101

Pour compléter de manière générale



P. Paradinas - 201

le cnam

Bibliography

➊ Books:

- ➋ Computer Security - Art and Science, Matt Bishop, Addison Wesley, 2003
- ➋ Security Engineering, Ross Anderson, Addison Wesley
- ➋ Cryptography and Data Security - Addison Wesley, Dorothy Denning, 1982
- ➌ Available on the web
- ➋ <http://www.schneier.com/>
- ➋ <http://www.electran.org/mobile-payments/>
- ➋ Identity Theft Resource Center (dashable.com)
- ➋ https://www.apple.com/business/docs/iOS_Security_Guide.pdf

P. Paradinas - 201

le cnam