micro and nanoelectronics
microsystems
ambient intelligence
image chain
biology and health

2009

Evaluation, Certification
Axes de R&D en protection

Dr Alain MERLE

CEA/LETI

Alain.merle@cea.fr

leti

MINATEC

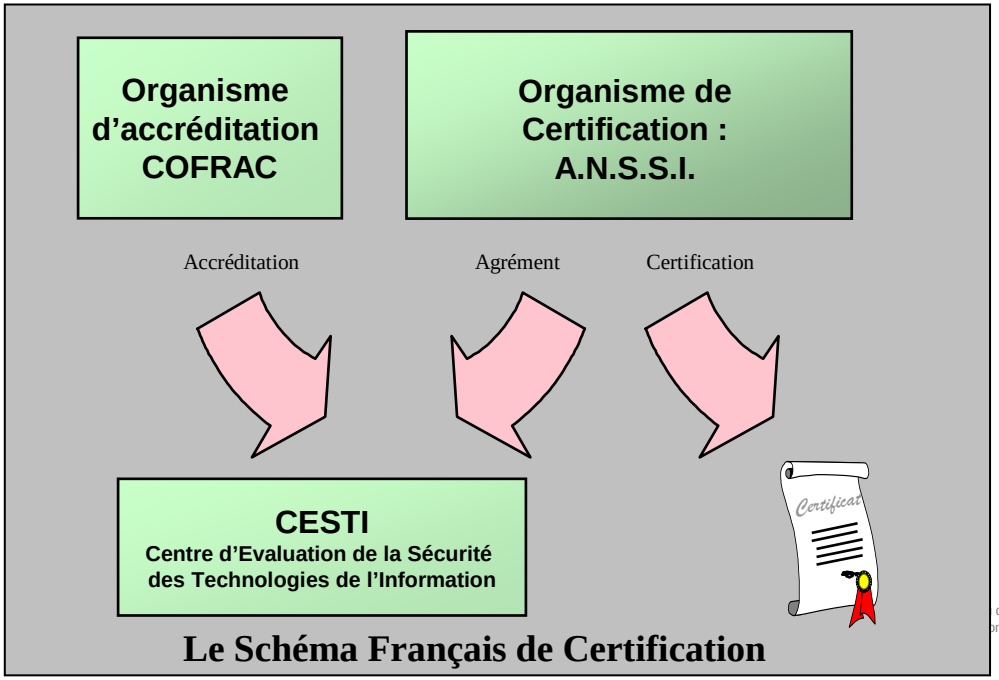
cea

Evaluation, Certification, Axes de R&D en protection

- Evaluation / Certification
  - Le Schéma Français de Certification
  - Les Critères Communs
  - CC et Attaques
  - Les principales techniques d'attaques
- Un peu d'histoire
- Axes de recherche au LETI

Le schéma Français de Certification

- Piloté par l'ANSSI
  - Accrédite des laboratoires
  - Emet les Certificats
- Laboratoires techniques indépendants (CESTIs)
  - Réalisent les évaluations
- Domaines d'agrément
  - Hardware (et logiciel embarqué)
  - Logiciel
- Niveaux d'agrément
  - Maîtrise des aspects semi-formels et Formels
  - EAL4/5 ou EAL7



Le Schéma Français de Certification

Les Critères Communs

Les Idées de base

- Description de la sécurité d'un produit
  - Spécifications sécuritaires argumentées
- Vérification de la conformité du produit à ses spécifications sécuritaires
- Tests (fonctionnels et attaques) du produit
- Vérification de contraintes environnementales

Common Criteria

- Une méthodologie d'analyse de la sécurité standardisée, objective et efficace (ISO IS 15408)
- Reconnaissance internationale des certificats
- En Europe, essentiellement utilisée pour les Cartes à Puces
  - Circuits Intégrés
  - Circuits avec logiciel embarqué

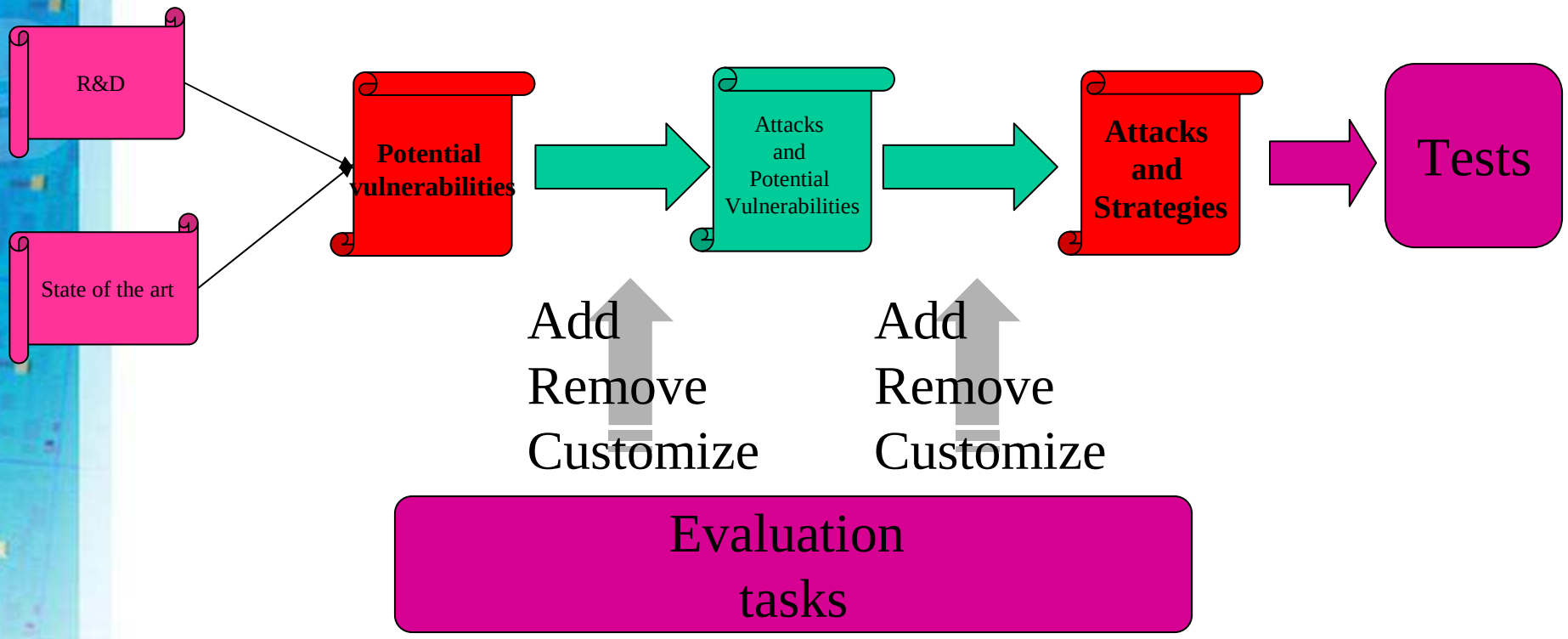
Evaluation des Cartes à Puce

- Common Criteria, EAL4+ (EAL5+ pour les IC)
  - Applications “haut de gamme” (bancaire, VITALE, etc)
  - Evaluation Boite Blanche
    - Accès à la conception
    - Accès au code source
    - Pour la vérification et les attaques
- Une table définissant le « attack potential »
  - Time, expertise, equipment, knowledge, …
  - La carte doit résister au maximum de ce qu’un attaquant peut faire
    - Toutes les attaques réalistes
    - Temps comparable à la durée de vie du produit

Quels tests

- Fonctionnels (Fonctions de Sécurité)
  - Conforme aux spécifications sécuritaires ?
- Attaques
  - Analyse de vulnérabilité indépendante
  - Challenge: Comment en 3/4 Mois
    - Couvrir l'ensemble des possibilités
    - Garantir (estimer ?) une durée de résistance supérieure ?

Stratégie de tests



L'évaluation sert à optimiser la durée des tests:

- En donnant à l'évaluateur des connaissances que le pirate devra acquérir
- En affinant les stratégies de test
- En limitant les tests

Attaque vs Stratégie d'attaque

- Observation (SPA, EMA, Cartographie)
  - Localiser (temps et espace)
  - Synchronisation
- Acquisition or Perturbation
- Traitement des données
- Répétition
  - 500K acquisitions pour une DPA
  - Perturbation: taux de réussite de l'ordre de 10^{-3} / 10^{-4}

La difficulté est plus d'attaquer les contre-mesures que d'appliquer une attaque connue

Attaques sur les Composants

- Physiques (Au niveau du Silicium)
  - Mémoires
  - Accès aux signaux internes
  - Modifications du circuit
- Observation: Side Channel Analysis
  - SPA, EMA, DPA, DEMA
- Perturbations: Générer des fautes
  - Exploitation des fautes (exemples)
    - IO errors (reading, writing)
    - Program disruption (jump, skip, change instruction)
    - Dynamic rewriting of the code
  - Cryptographie (DFA)
- Attaques sur le logiciel embarqué
  - Protocole, overflows, erreurs, …

Exigences pour les CESTIs

- **Compétences spécifiques** en attaques dans le domaine
  - Connaissance de l'Etat de l'art (pas toujours/entièrement publié)
  - R&D en Attaques
  - Multi-competences
    - Cryptographie, microelectronique, traitement du signal, mesures, , lasers, etc
  - Equipements de la micro-électronique
    - MEB, FIB, plasma etching, chemical etching, …
  - La sécurité est un secteur en évolution constante et rapide
    - Fort background et activités suivies
- Réduire l'incertitude
  - Qualité, Sécurité, Formation, etc

En résumé

- L'Evaluation est
  - Un processus Rigoureux et Normalisé
  - Mais les attaques requièrent une compétence humaine
  - **L'objectivité ne peut être totale** (malgré une uniformisation européenne)
- Conformité vs Résistance
  - L'évaluation sert (aussi) à optimiser les tests
  - Ce n'est pas qu'un processus documentaire lourd
- L'évaluation/Certification a été un **moteur très efficace** pour **l'amélioration de la résistance** des composants ces dix dernières années

CC: Norme ou Cadre de travail

- Majoritairement utilisés pour les Cartes à Puce
- Mais de nombreux travaux ont été nécessaires (et continuent) pour que ce process soit efficace

Supporting Documents related to Smart Cards and similar devices

Document number	Document title	Class
2006-06-001	Rationale for Smart cards and similar devices	
CCDB-2006-04-001	Guidance for smartcard evaluation v1-3	Guidance
CCDB-2009-03-001	new Application of Attack Potential to Smartcards v2-7	Mandatory
CCDB-2009-03-002	new Application of CC to Integrated Circuits v3-0	Mandatory
CCDB-2007-09-01	Composite product evaluation for Smartcards and similar devices v1-0	Mandatory
CCDB-2007-09-02	ETR-template lite for composition v1-0	Guidance

Evaluation, Certification, Axes de R&D en protection

- Evaluation / Certification
  - Le Schéma Français de Certification
  - Les Critères Communs
  - CC et Attaques
  - Les principales techniques d'attaques
- Un peu d'histoire
- Axes de recherche au LETI

1996 – 2009: La sécurité

Un circuit de 12 ans est du niveau d'un TP d'étudiants

Et Alors ?

- Contexte: Les produits évoluent
  - Durée de vie longue: e-Id, e-passport
- Vue négative
  - Y a-t-il de bonnes raisons pour que les 10 prochaines années soient différentes des 10 précédentes ?
- Vue positive
  - A chaque attaque correspondent des contre-mesures efficaces (tout ce qui est vu n'est plus à voir !)
  - Le niveau s'est grandement amélioré (Accroissement de l'effort d'attaque très significatif)
  - Peu d'idées nouvelles

La résistance absolue: un mythe ?

- Tous les schémas crypto sont basés sur un secret
  - L'accès à ce secret fait tomber le système
- La résistance théorique évolue rapidement
  - Loi de Moore de la microélectronique
  - DES, TDES, AES, RSA key length, Hash fns
- Le hardware ne peut être **LA** solution parfaite
  - C'est un objet physique donc attaquable !
  - Nouvelle attaques découvertes chaque jour
    - DPA, EMA, DFA, Laser, …
  - Questions sur la durée de vie
    - Un circuit de 12 ans d'âge est un cas d'école

L'hypothèse de faire face à une attaque réussie doit être prise en compte

Challenge : Meilleure sécurité

Meilleure Resistance

- Meilleure durée de vie
  - > 10 years
  - Casser le cycle Attaque / Défense
  - Architectures sures
- Du Circuit au Microsystème
  - Auto-surveillance
  - Capteurs, Energie, etc

Nouvelles Approches

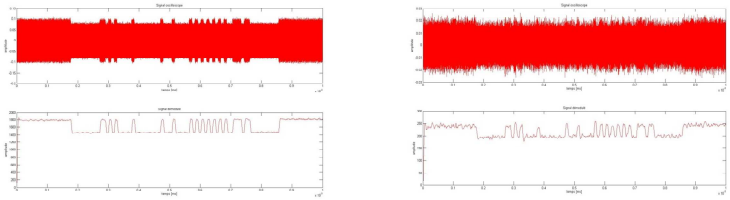
- Sécurité Multi-Barrières
  - Authentification physique
  - Compromission partielle
- Processeur de sécurité
  - Politiques de sécurité pour la détection/réaction
  - Processeur d'audit

Contactless: Une problématique spécifique

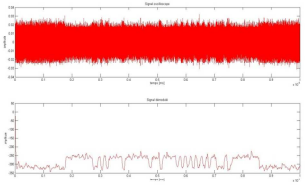
Contactless: Une problématique spécifique

Eavesdropping

Forward link type B : 15 cm antenna at 8 m, 16 m and 50 cm antenna at 22m

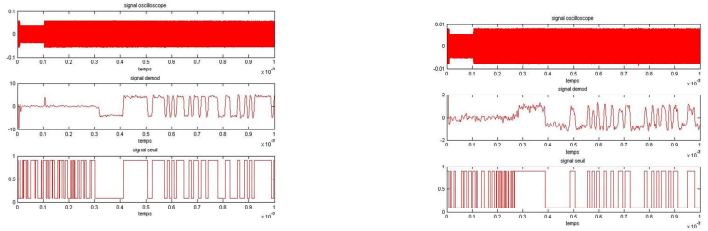


- Eavesdropping forward link: Reader to card
- Type B (A « easier » than B)
  - Diameter = 15 cm ⇨ 18m
  - Diameter = 50 cm ⇨ 22m
  - Whip type antenna ⇨ 4m



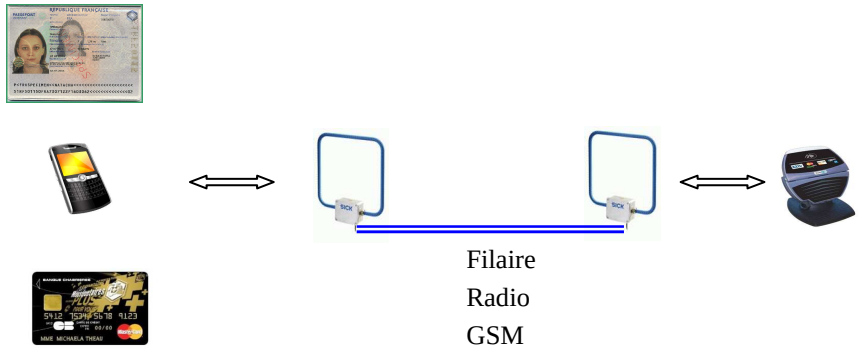
Eavesdropping

Return link type B : ISO 10373-6 antenna at 1 m and 50 cm at 3.5 m



- Eavesdropping return link: Card to reader
  - Type B (quite same for type A)
    - Antenna diameter = 15 to 20 cm ⇨ 3 to 3.5 m
    - Antenna diameter = 40 to 50 cm ⇨ 4 m

- ➢Ecoute à distance
- ➢Activation non contrôlée
- ➢Relais



Filaire
Radio
GSM

Challenge: Et la disponibilité ?

- Critères de la Sécurité
  - Confidentialité
  - Intégrité
  - Disponibilité
- Aujourd'hui la disponibilité n'est pas adressée
  - Exemple: Effacement des mémoires en cas d'attaque
- Attaques en Déni de Service
  - Activisme / Terrorisme
  - Passage en mode à capacité réduite
  - Des exemples existent ……
  - Nouvelles architectures / Nouveaux schémas nécessaires

Conclusion

- Personne n’est parfait ….
  - Le Hardware est une bonne solution … mais des limitations existent
  - Tout Schéma limité à la résistance d’un seul élément est limité
- Des pistes existent et doivent être explorées
- Attention aux nouveaux schémas d’attaque (Déni de Service, Destruction)


micro and nanoelectronics
microsystems
ambient intelligence
biology and health
image chain
Merci de votre attention
Questions ?
Loyalty
Entrepreneurship
Team work
Innovation
leti
MINATEC
cea