



Techniques d'attaques des microcircuits par pénétration partielle

Bruno KEROUANTON – Responsable SNT - CISSP



CLEARCHANNEL



Quels buts, quelles motivations ?

- Enjeux de plus en plus importants
 - TV satellite, cartes bancaires, etc...
 - Données personnelles stockées
- Source d'innovations technologiques
 - Réduction du coût de R&D
 - Contrefaçon, vol de brevets



Techniques d'attaque des microcircuits

Invasives

Non invasives

Semi-invasives



Attaques invasives

Rétro-ingénierie :

- Puce mise à nue chimiquement ou mécaniquement.
- Analyse complète de la conception.
- Positionnement de microsondes sur les bus de données et registres.
- Utilisation de faisceaux d'ions pour modifier la structure du microcircuit.



Attaques non-invasives

- N'altère ni le microcircuit ni son enrobage.
- Utilisation de « failles » de conception de nature physique :
 - Micro-coupures et micro-surtensions
 - Changement de la température du circuit
 - Modification du signal d'horloge
 - Mesure précise de la consommation ou des temps de réponse (voir MISC !)



Attaques semi-invasives

Pénétration partielle par faisceau laser :

- Puce mise à nu chimiquement...
- Mais sans altérer la couche de protection.
- Mise à 0 ou 1 de bits par laser :
 - Suppression de la protection du microcode.
- Lecture de bits par laser :
 - Récupération de clefs privées RSA !



Avantages et inconvénients

	Attaques Invasives	Attaques semi-invasives	Attaques non-invasives
Freins	Onéreux Complexe		Empirique Long à réaliser
Motivations	Efficace	Bon marché Efficace	Très bon marché Simple



Quelques microcircuits vulnérables

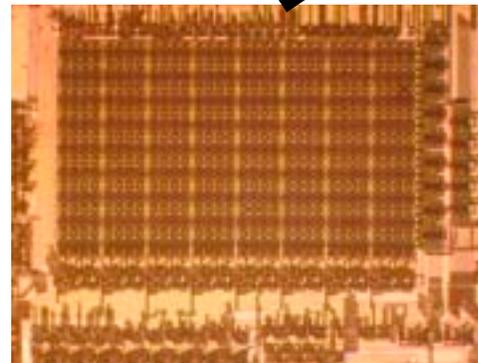
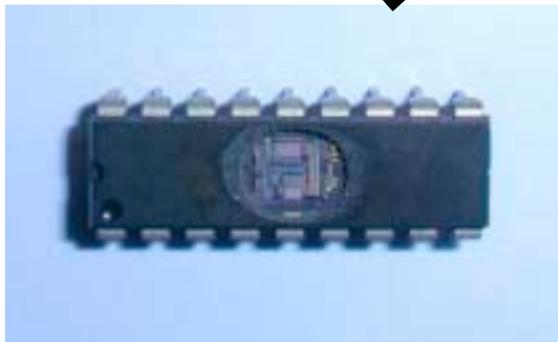
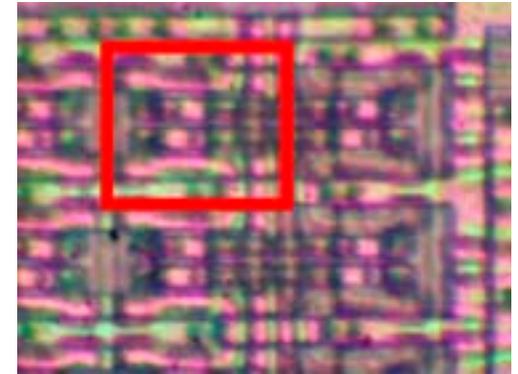
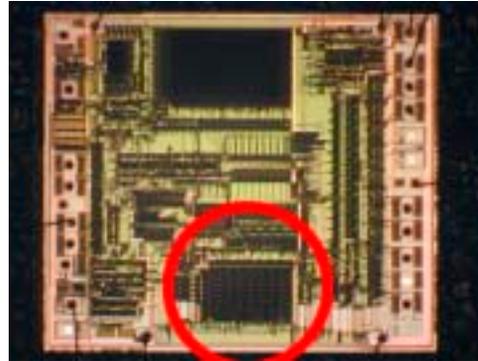
Mémoires : RAM, SRAM, EPROM, EEPROM,
FLASH, etc...

(peut nécessiter un « gel » du contenu par
cryogénie ou arrêt du signal d'horloge).

Microcontrôleurs : la plupart des circuits courants
(MC68HC05, MC68HC11, PIC 16C84, AT89C51,
etc...)



Exemple



Mesures de protection

- Nouvelle génération de microcircuits
 - Chiffrement « simple » des bus et mémoires
 - Dissimulation optique des modules
 - Capteurs d'attaques (température, rayonnements, etc...)
 - Circuits à horloges indépendantes
 - Circuits à logique asynchrone



Conclusion

L'attaquant est capable de tout...

... et surtout de ce que l'on n'a pas prévu !

➔ imaginer le pire pour avoir le meilleur



Références, remerciements

Je remercie chaleureusement :

Sergei P. Skorobogatov et **Ross Anderson**
(Tamper Lab, University of Cambridge)

Références :

- Optical fault induction attacks.
- On a new way to read data from memory.
- Improving SmartCard security using self-timed circuits.
- Balanced self-checking asynchronous logic for smart card applications.

Liens internet :

<http://www.cl.cam.ac.uk/~sps32>

<http://www.cl.cam.ac.uk/~rja14>

