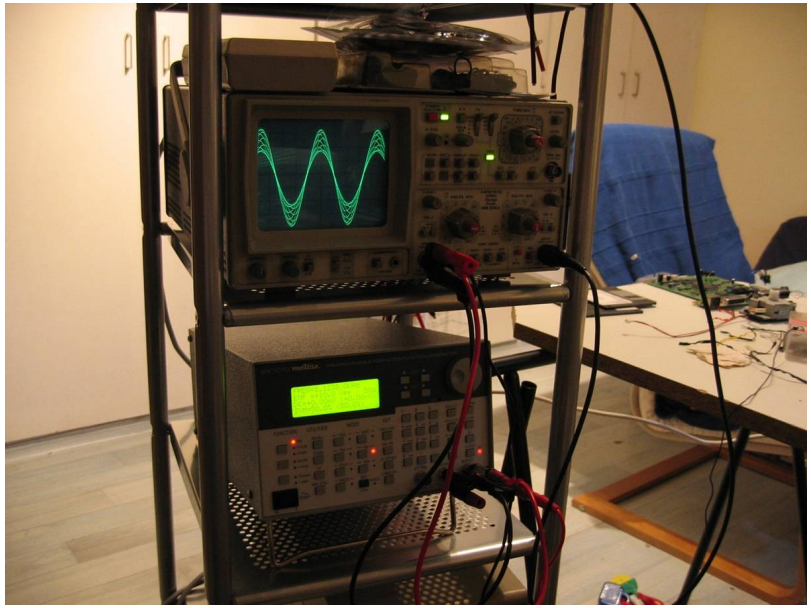
# Reverse engineering materiel

SSTIC 2004

Rump sessions

bruno@kerouanton.net



# Introduction

- De plus en plus de systèmes embarqués, de périphériques, de nomades etc...
- Comment être certain que la sécurité de ces équipements soit efficace. Peut-on se fier aux dires du constructeur ?

# Analyse materielle

- Peut etre long et fastidieux, donc on doit « optimiser ».

- Valable uniquement pour des cas précis, on se limitera alors aux seuls composants ou fonctions méritant d'être testés (crypto processeurs, systèmes d'entrées-sorties, générateurs d'aléas, etc...) afin de gagner du temps.

# Analyse electronique

Nécessite :

- des connaissances en électronique,
- du matériel de laboratoire,
- et l'accès physique aux circuits électroniques.

Exemples dans MISC : Récupération de clefs RSA par analyse de consommation ou de timing...

# Methode courante

- Inspection visuelle des circuits électroniques,
- repérage des composants pour en déterminer la fonction,
- application de signaux précis / anomalies à des endroits précis afin d'observer le comportement du système.

# Outillage

- Moins de 1500 euros (achats d’occasion)
- Oscilloscope a memoire, analyseur logique, generateur d’impulsions, generateur de signaux arbitraires, bombe de refroidisseur, databooks, experience…

# Conclusion

Pas tres onereux (accessible au particulier), methode efficace si on a du temps et des connaissances en electronique.

De plus en plus de cas de reverse engineering materiel publies.