Le cassage de DES, édition non expurgée

- Informatique - Sécurité Informatique -

Date de mise en ligne : samedi 30 septembre 2006

Spyworld Actu

DES étant en voie de disparition notamment au sein de l'administration américaine, l'embargo sur le code source de l'algorithme de cryptage est enfin levé... embargo qui ne servait plus à rien depuis belle lurette, doit on préciser. Cette levée du secret donne donc à l'Electronic Frontier Foundation la possibilité d'éditer en intégralité son ouvrage « Cracking DES, Secrets of Encryption Research, Wiretap Politics & Chip Design, How federal agencies subvert privacy ». Trois chapitres manquaient à l'édition officielle américaine, chapitres qui circulaient en Europe depuis longtemps déjà. Outre l'aspect doctoral et éducatif de l'ouvrage à l'attention des mathématiciens et spécialistes de la cryptographie, l'on peut admirer un superbe hack du fond de panier d'une machine Sun, dans le seul but de « casser du DES ». Le plan est manifestement tracé sous Orcad, un mail auprès de l'EFF est donc nécessaire pour les plus passionnés souhaitant générer le fichier de routage au format gerber.

Post-scriptum :

http://www.reseaux-telecoms.net/act...