Wep cracking…

Frnog 6

01 avril 2004

Cyril Leclerc

Agenda

Le wep est mort (encore)

- Nécrologie du wep
- Outils actuels passifs

Deuxième partie

- Outils actifs
- PEAP…

Le wep est mort (encore)

Wep cracking

Chronologie d'une mort annoncée (un peu tôt)

- **Octobre 2000, premier papier sur les faiblesses du wep…**

http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

- **Aout 2001, attaque FMS qui sera implémenté dans la plupart des outils (Scott Fluhrer, Itsik Mantin, and Adi Shamir):**

http://www.cs.umd.edu/%7Ewaa/class-pubs/rc4_ksaproc.ps

- **Ce même mois (Aout 2001), le monde découvre airsnort:**

http://www.wired.com/news/wireless/0,1382,46187,00.html

- **Dans la foulée, les vendeurs commencent à filtrer les IV faibles sur les nouveaux produits commercialisés… Ceci rend Airsnort inopérant dans la plupart des cas…**

Chronologie d'une mort annoncée (un peu tôt)

- **Mar. 2002 dashb0den distribue une attaque type FMS optimisée et plus efficace qu'Airsnort, elle reste cependant dépendante des IVs faibles de plus en plus rares…**

- **14/11/2002 dashb0den toujours diffuse un outil permettant de reinjecter des paquets capturés afin d'augmenter le traffic…**

- **07/2004 Korek diffuse un bout de code permettant de casser une clé wep en disposant de 10x-20x moins de paquets qu'airsnort (et sans IVs faibles !)**

- **08/2004 sortie de weplab, qui implémente le code de Korek dans un outil grand public…**

- **Le même mois, Christophe Devine diffuse les premières version d'aircrack qui sonne définitivement le glas du wep… Cet outil permet de casser une clé wep avec 98% de reussite sans le moindre IVs faibles en disposant de 400-1000k paquets…**

Outils passifs classiques

Statistiques (source SF/ Michael Ossmann):

Data Packets	Weak IVs	Unique IVs	128 bit Cracking Time in Seconds						
			aircrack	aircrack (4)	AirSnort	WepLab	WepLab (95)	WEPCrack	dwepcrack
23457438	8560	16775533	Failed	245	92	Failed	244	Failed	Error
21016149	1807	16775167	Failed	249	41	Failed	247	Failed	Failed
19584364	9340	16275925	Failed	230	114	Failed	229	Failed	Failed
15690079	8694	12860342	Failed	184	90	Failed	179	Failed	Error
15628308	5505	12361369	Failed	176	70	Failed	174	Failed	Failed
11743639	8473	11743639	Failed	154	69	Failed	153	Failed	Error
11739339	3037	11693841	Failed	150	Failed	Failed	151	Failed	Failed
7829104	1001	5031233	Failed	74	Failed	Failed	77	Failed	Error
7799213	5225	7779299	Failed	87	37	Failed	101	Failed	Failed
4175159	1554	4069824	52	51	Failed	Failed	54	Failed	Failed
3914568	767	3914568	Failed	Failed	Failed	Failed	Failed	Failed	Error
3914553	3958	3914553	48	49	Failed	Failed	56	Failed	Error
3884657	1490	3864743	48	46	Failed	Failed	52	Failed	Failed
978652	986	978652	Failed	Failed	Failed	Failed	11	Failed	Error
978633	371	978633	Failed	12	Failed	Failed	13	Failed	Error
977219	264	974902	Failed	9	Failed	Failed	13	Failed	Failed
684992	143	684992	8	8	Failed	Failed	11	Failed	Error
683605	238	681288	Failed	18	Failed	Failed	13	Failed	Failed
587184	117	587184	Failed	27	Failed	Failed	Long	Failed	Error
489293	103	489293	8	7	Failed	5	5	Failed	Error
489286	115	489286	15	16116	Failed	Failed	Long	Failed	Error
391465	78	391465	5	13	Failed	Failed	Long	Failed	Error
391433	78	391433	Failed	6	Failed	Failed	6	Failed	Error
293596	65	293596	Failed	5	Failed	Failed	Long	Failed	Error
293579	65	293579	Failed	Failed	Failed	Failed	Failed	Failed	Error

Table 1. 128 bit WEP Cracking Times (in seconds).

Outils passifs classique

Démonstration avec:

- Capture avec kismet sur un wrt54g

- Aircrack sous linux

Outils actifs

Wep cracking

Outils actifs

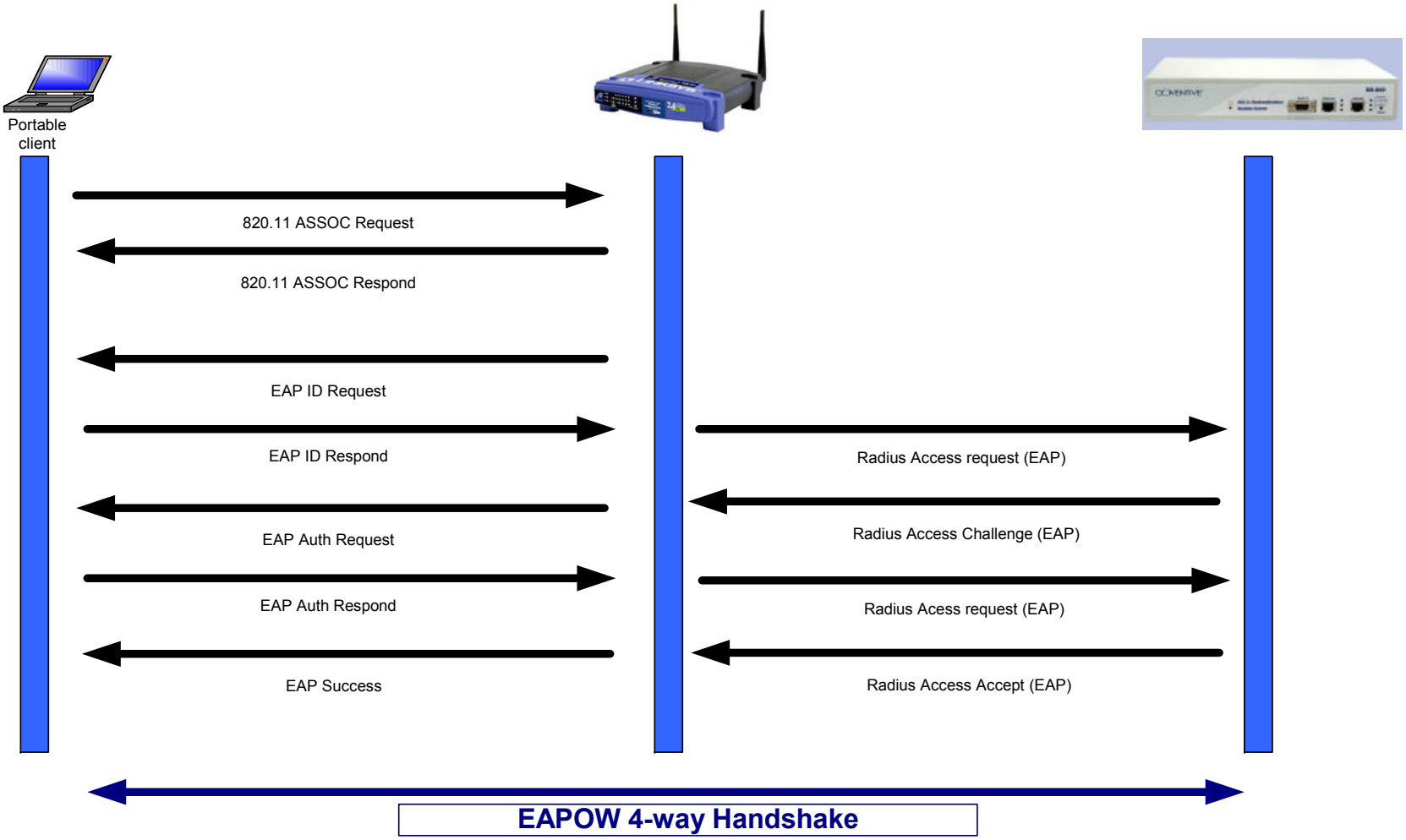
Avant, reinj sur Openbsd 2.6 avec un kernel patché…

Maintenant aireplay (aircrack), permet de reinjecter les paquets avec un linux et une carte prism2 (et le driver hostap correctement patché)

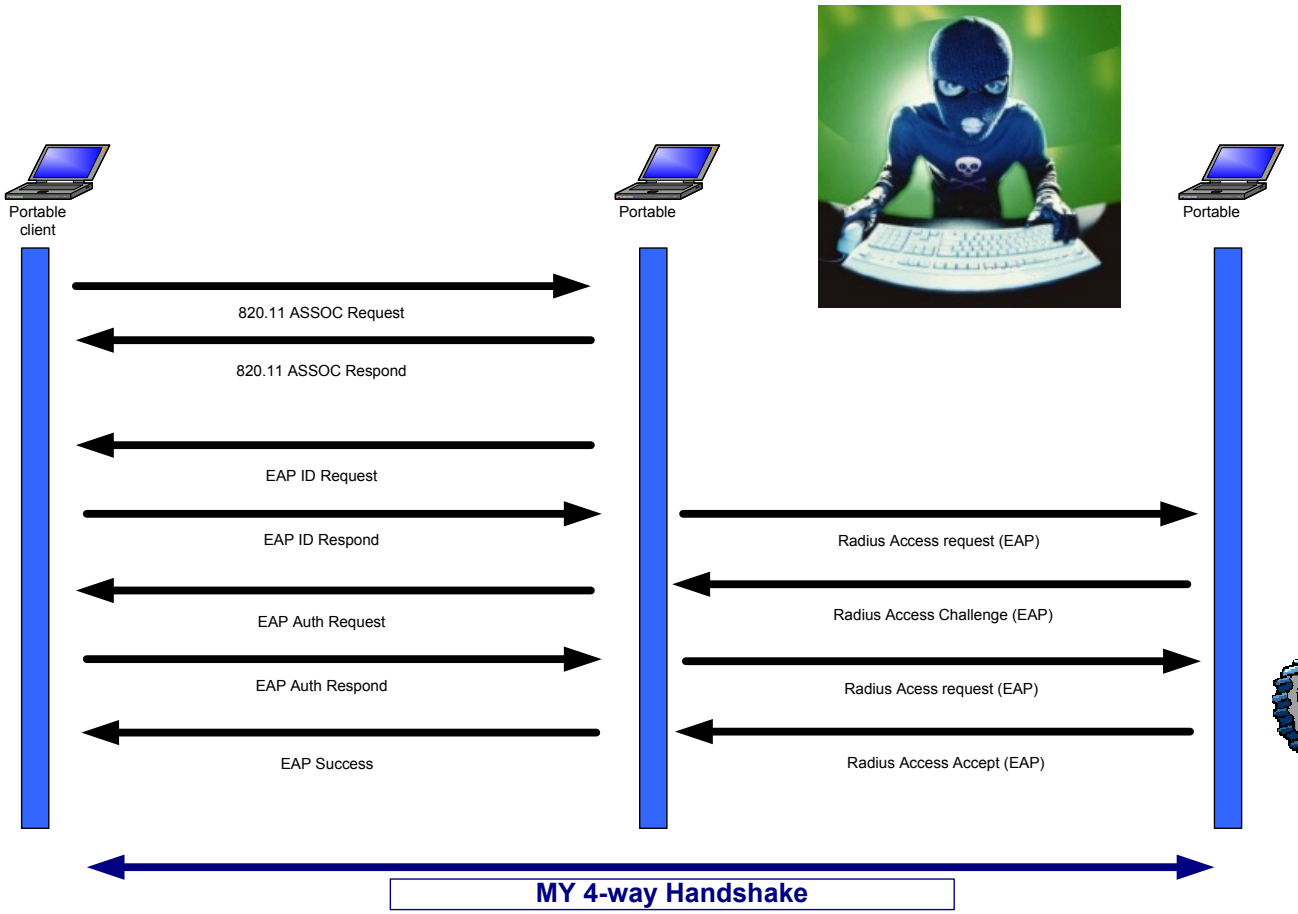
Cette attaque nécessite tout de même 2 cartes (une pour injecter, une pour sniffer)

Demo

PEAP / Fonctionnement



PEAP / Man in the middle



Un petit Dico Ou

Stockage du hashcode pour déchiffrement ultérieur

Contact

Cyril Leclerc

Mél : cleclerc@arseo.com

01/04/2005

ARSeO

8 rue de Valmy

93100 Montreuil

France

www.arseo.com