NOTE TECHNIQUE 21071998

Rédacteur : Élie AOUAD

Analyse des erreurs de Personnalisation pour Etebac5 V2.1

1. Introduction

Cette note technique, essaie d'analyser les raisons d'erreurs de personnalisation des cartes DXP pour Etebac5 V2.1, en se basant sur des analyses statistiques de certaines cartes testées.

EASEiT a testé 4 cartes DXP et un jeu de cartes M9. Un seul mapping d'une carte DXP était connu, ainsi que les cartes M9 qui contiennent les secrets sous la forme des composantes premières.
3 cartes DXP sur 4 possèdent des erreurs. La carte M9 a sa 4ème clé secrète erronée.

Un clé est considérée bonne si la l'opération de signature est l'inverse de l'opération publique correspondant à la clé secrète.

2. Résultats

Carte	Numéro clé	Début du modulo	début p dans carte	début q dans carte	sqrt(début N)	Etat de clé
DXP1	0	F6A9			FB	NOK
	1	AF62				OK
	2	8274				OK
	3	8F00				NOK
DXP2	0	C703				OK
	1	EAD7				OK
	2	E875				OK
	3	9188				NOK
DXP3	0	D4A6				OK
	1	E4A4				OK
	2	F68A			FB	NOK
	3	B360				NOK
DXP4	0	DD09	F3	E8	ED	OK
	1	C055	F7	C7	DD	OK
	2	8F56	EA	9C	BF	OK

	3	C89A	FF	C9	E2	OK
M9	0	D074	E1	EC	E7	OK
	1	D11F	F7	D7	E7	OK
	2	E3AC	FF	E3	F1	OK
	3	F2AE	80B2	**E2BD**	F9	NOK
Moyenne		***C7..***				

3. Analyses

2.1 La moyenne du début de modulo sur les diverses clés générées est de C7. Ce qui est statistement très bon, car la moyenne théorique des modulos est de C7FFFFFF...FF.

2.2 En analysant bien les clés M9, on remarque que p> q 2 fois/4. Ce qui est statistiquement bon.

2.3 La 4ème clé du jeu M9 est erronée car la composante q a été sauvegardée sur 64 octets au lieu de 65. En effet en divisant F2AE.... par 80B2 on tombe sur q = 1E2BD. Un patch manuel du bit le plus significatif manquant à 1 corrige l'erreur sur le jeu M9. A partir de cette valeur de composante on peut donc affirmer que le générateur de clés M9 peut donner des composantes sur 513 bits. Si c'est le même générateur qui est utilisé pour les cartes DXP, il faut s'attendre donc à des composantes sur 513 bits.

2.4 Pour qu'une clé secrète d'une carte DXP fonctionne normalement il faut que p > q, et que les composantes des restes chinois soient conservés dans l'ordre suivant:
Deux octets entête, Taille p, p, taille sp, sp, taille q, q, taille sq, sq, taille u, u.
Chaque taille est sur un octet.

Une analyse du répertoire des clés dans les cartes DXP, indiquent des tailles de conservation des composantes sur 327 octets; **soit une taille de 64 octets (512 bits) par composante.**

Revenons un peu aux statistiques, et à la définition du modulo N = p * q, ainsi qu'au générateur de la carte Vasco qui génère une composante ayant la moitié de la taille du modulo, donc au minimum de 512 bits de taille. p et q se situent aux alentours directs de leur moyenne géométrique à savoir la racine carrée du modulo. La probabilité d'avoir une composante 513 bits est d'autant plus importante que la moyenne géométrique ou le modulo sont plus importants. Sans rentrer dans les détails mathématiques pour aboutir à la probabilité exacte, on peut considérer que pour un modulo commençant par F,la probabilité d'avoir une composante de 513 bits est très forte. **On peut donc s'attendre à une probabilité forte de composantes à 513 bits (65 octets) sur 1/8 à 1/16 des composantes générées.** Ce qui correspond bien aux résultats DXP1/Clé 0 et DXP3/Clé 3 dont les modulos commencent par F6. En tenant compte des cartes récemment personnalisées (3cartes testées par EASEiT, 2 cartes par ailleurs), et sans tenir compte de la 4ème clé on peut dire qu'on a deux composantes à 513 bits (du fait de l'erreur sur la clé) sur 30 (6 composantes par carte); donc un taux de 1/15.

2.5 Reste le problème de la 4ème clé des cartes DXP. Elle est systématiquement erronée dans 3 cartes sur 4. Les trois mauvaises cartes ont été personnalisées au mois de juin. La bonne date de mai. Par ailleurs deux autres cartes récentes livrées ont aussi la quatrième clé erronée. Ce qui peut indiquer une erreur systématique sur la 4ème clé sur les cartes personnalisées.

De plus les cartes DXP1 et DXP3 partent en timeout sur l'exécution de la signature sur la quatrième clé ce qui peut indiquer une erreur de stockage des composantes sur la DXP probablement au niveau des tailles des composantes.

L'erreur systématique sur la 4ème clé peut avoir des interprétations diverses sans pouvoir décerner exactement l'origine de cette erreur du fait que la mapping des cartes DXP1 à DXP3 n'existe pas:

- ?? génération systématique de composante à 513 bits, (un autre générateur est utilisé pour la 4ème clé??)
- ?? écriture erronée et donc mauvais stockage car la 4ème clé se trouve à la fin??
- ?? le hasard des choses?

4. Conclusions

4.1 Erreur de stockage de la composante de la 4ème clé sur la carte M9.

4.2 Erreurs de stockage sur certaines clés 0, 1, 2 du fait que certaines composantes sont générées sur 513 bits, et que le répertoire indique un stockage systématique sur 64 octets (512 bits).

4.3 Pour la 4ème clé systématiquement erronée, il faut une analyse plus avancée.

5. Et les Causes réelles furent…

Les causes réelles furent pour les clés 1,2,3 comme indiqué par EASEiT (génération sur 513 bits au lieu de 512 bits pour les composantes).
Quant à la 4ème clé elle est erronée à cause d'un débordement de pile!!