p1b7l4899s0-.pdf

From: Conus Joël
Sent: Wednesday, November 21, 2001 5:23 PM
To: 'Guggenheim, Alan'; Groux Cédric; Gaillard, Christophe; Nicolas Christophe; Kudelski Henri; Gee, JJ
Subject: RE:

*** PGP Signature Status: good
*** Signer: Joël Conus <conus@nagra-kudelski.ch>
*** Signed: 11/21/2001 5:22:00 PM
*** Verified: 11/21/2001 7:59:58 PM
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***

This file contains 6 HU ROM dumps. I think we have to view H and HU as families which would be compared to DNASP2 and DNASP3 (Aladin) in our system. I don't know if they have to use simulcrypt though.
As far as I can tell these dumps are full dumps of the ROM of different HU cards. I've been able to (partly) check their validity by making a comparison with a previously released HU ROM dump. The HU ROM code take 16KB while the HU EEPROM takes 4KB.
Now I don't know why they called this file HU ROM "keys"... there might be common keys in there but most keys (personalized keys that is) are stored in the EEPROM. BTW most of the EEPROM is encrypted (XORed) with an 8 bytes key that seems unique for each card.
Anyway, the fact that most types of HU ROMs have now been published will boost the glitch attacks and the market behind. This will especially put the HU unlooper on the market at an affordable price (I've read that the HU unloopers cost about USD 5K now).
This is highly valuable information for the DSS community.

-Joel

> -----Original Message-----
> From: Guggenheim, Alan [mailto:alan.guggenheim@nagrastar.com]
> Sent: mercredi, 21. novembre 2001 04:48
> To: Joel Conus (E-mail); Cedric Groux (E-mail); Gaillard, Christophe; Nicolas, Christophe; Kudelski, Henri; Gee, JJ; Guggenheim, Alan
> Subject: FW:
>
>
>
>
>
> *** PGP Signature Status: good
> *** Signer: Alan A. Guggenheim <guggenheim@nagra.com>
> *** Signed: 21.11.2001 04:47:03
> *** Verified: 21.11.2001 16:51:12
> *** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***
>
> This is the file mentionned by Renee in her email.
>
> We need to get familiar with this. What's the value?
>
> Thanks
>
> Alan A. Guggenheim
> CEO
> Nagra|Star
> Alan.Guggenheim@NagraStar.com <mailto:Alan.Guggenheim@NagraSta

CONFIDENTIAL Case No. SA CV03-950 DOC (JTL)

CASE NO.
SA CV 03-950 DOC (JTLx)
ECHOSTAR SATELLITE CORP., et a
vs.
NDS GROUP PLC, et al.
DEFENDANT'S EXHIBIT 816
DATE _____ IDEN.
DATE _____ EVID
BY _____
Deputy Clerk

p1b7l4899s0-.pdf

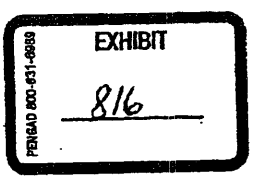
From: Conus Joël
Sent: Wednesday, November 21, 2001 5:23 PM
To: 'Guggenheim, Alan'; Groux Cédric; Gaillard, Christophe; Nicolas Christophe; Kudelski Henri; Gee, JJ
Subject: RE:

*** PGP Signature Status: good
*** Signer: Joël Conus <conus@nagra-kudelski.ch>
*** Signed: 11/21/2001 5:22:00 PM
*** Verified: 11/21/2001 7:59:58 PM
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***

This file contains 6 HU ROM dumps. I think we have to view H and HU as families which would be compared to DNASP2 and DNASP3 (Aladin) in our system. I don't know if they have to use simulcrypt though.
As far as I can tell these dumps are full dumps of the ROM of different HU cards. I've been able to (partly) check their validity by making a comparison with a previously released HU ROM dump. The HU ROM code take 16KB while the HU EEPROM takes 4KB.
Now I don't know why they called this file HU ROM "keys"... there might be common keys in there but most keys (personalized keys that is) are stored in the EEPROM. BTW most of the EEPROM is encrypted (XORed) with an 8 bytes key that seems unique for each card.
Anyway, the fact that most types of HU ROMs have now been published will boost the glitch attacks and the market behind. This will especially put the HU unloopers on the market at an affordable price (I've read that the HU unloopers cost about USD 5K now).
This is highly valuable information for the DSS community.

-Joel

> -----Original Message-----
> From: Guggenheim, Alan [mailto:alan.guggenheim@nagrastar.com]
> Sent: mercredi, 21. novembre 2001 04:48
> To: Joel Conus (E-mail); Cedric Groux (E-mail); Gaillard, Christophe; Nicolas, Christophe; Kudelski, Henri; Gee, JJ; Guggenheim, Alan
> Subject: FW:
>
>
>
>
>
> *** PGP Signature Status: good
> *** Signer: Alan A. Guggenheim <guggenheim@nagra.com>
> *** Signed: 21.11.2001 04:47:03
> *** Verified: 21.11.2001 16:51:12
> *** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***
>
> This is the file mentionned by Renee in her email.
>
> We need to get familiar with this. What's the value?
>
> Thanks
>
> Alan A. Guggenheim
> CEO
> Nagra|Star
> Alan.Guggenheim@NagraStar.com <mailto:Alan.Guggenheim@NagraStar.com>



> Tel: +1 (303) 706-5707
>
>
>
>
> -----Original Message-----
> From: Gaillard, Christophe
> Sent: Tuesday, November 20, 2001 7:59 PM
> To: Guggenheim, Alan
> Subject:
>
>
>
>
>
>
> lw floppy que tu m'as filé.
> ca a l'air des dump de rom code DTV, pas juste des cles.
>
>
> ----------
> Christophe Gaillard - CAS Operations Manager Nagrastar Tel. +1 303 706
> 5703 Fax. +1 303 706 5719
>
>
>
>
> *** END PGP DECRYPTED/VERIFIED MESSAGE ***
>
>

*** END PGP DECRYPTED/VERIFIED MESSAGE ***