Informationsläckage i GPG/PGP

Vem är jag?

- Forskare på FOI 2003 ->
- IT-säkerhet, specialintresse IT-forensik
- Statens Kriminaltekniska Laboratorium (SKL) 2010-09 – 2013-12

Demo Informationsläckage

- Vad?
  - Komprimerad klartext eller inte?
- Hur?
  - 5 textfiler (38-64 MiB)
  - Zippa dem
  - Kryptera alla filer med AES256
  - Anonymisera (filnamn = SHA1)
- När?
  - Nu!

RFC 4880 (OpenPGP)

- (4.2.2.4) Partial Body Lengths
  - 1 Byte, datalängd = 2^(bytevärde-224)
  - Här; 2^(0xED-0x1F)=2^(237-224)=2^13=8192
- ”An implementation MAY use [PBL]” (RFC 4880, sid. 15)
- GPG gör det för tillräckligt stora filer

Tack för mig!

Martin Karresand, FOI

martin.karresand@foi.se, martin@filecarving.net

013-378543 eller 013-378081