

Crypto is the Chicken Soup in Plain English



[Peter Gutman](#), „computer scientist in the Department of Computer Science at the University of Auckland, Auckland, New Zealand“, [hat etwas publiziert](#) (pdf, via [Fefe](#)) über die Schwachstellen gängiger kryptografischer Implementationen und das Computerproblem, das zwei Ohren hat und vor einem Monitor sitzt.



Er lässt sich unter anderem aus über Amazon Kindle 2, Motorola und Samsung Galaxy Handys, Nikon und Canon Kameras, Android code signing, iPhone/iPad/iOS („lets of security measures, too many to cover here“), Windows 8 UEFI (das ärgert mich sowieso schon seit langem) usw..



Natürlich ist jemand wie Gutman, [der sich wirklich auskennt](#), kein Defätist. Er macht nur noch einmal klar, dass man nicht auf Technik oder Software allein vertrauen sollte: Vertrauen ist gut, Kontrolle ist aber besser.

Auf jeden Fall lesenswert, auch wegen des schwarzen Humors und der lässigen Sprache, den man auf Folien eines Deutschen zu einem solchen Thema so nicht finden würde.

