Bezpieczne poÅ‚Ä…czenia?

Zmieniony 09.11.2013.

Wiadomo, Å¼e Ed Snowen co jakiÅ› czas podaje nam garÅ›Ä‡ ogólnych faktów na temat poufnoÅ›ci naszych E-maili, danych i
Tym razem Snowden zaszokowaÅ, wszystkich prawdziwÄ… bombÄ…. OtóÅ¼ standardowe programy do szyfrowania,
(prawdopodobnie SSL) sÄ… skopane juÅ¼ na etapie projektowania, Å¼eby NSA mogÅ‚o sobie pooglÄ…daÄ‡ conieco.
W czym problem?

O ile dobrze mi wiadomo, algorytm AES jest standardem w dziedzinie algorytmów szyfrowania, przy którym majstrowaÅ‚o m
in. NSA. Gdy wyÅ‚aniano algorytmy szyfrujÄ…ce na zasadzie konkursu, szyfr Rijndael staÅ‚, siÄ™ standardem, ze wzglÄ™du n
optymalne wywaÅ¼enie miÄ™dzy mocÄ… szyfrowania, a szybkoÅ›ciÄ…, PrzegraÅ‚ z nim ciut wolniejszy, otwartoÅºródÅ‚owy T
który podobno nie zostaÅ‚ nigdy zÅ‚amany. Jako Å¼e AES jest standardem, ja osobiÅ›cie postanowiÅ‚em uÅ¼ywaÄ‡ do
szyfrowania zarówno twofish jak i AES, MoÅ¼e to coÅ› pomoÅ¼e. Poza tym moÅ¼liwe, Å¼e jak SSL jest skopany,
naleÅ¼aÅ‚oby szyfrowaÄ‡ dane jeszcze przed wysyÅ‚aniem czegokolwiek, co uniemozliwi/utrudni deszyfrowanie na etapie
wysyÅ‚ki danych. Niestety, jak zwykle Snowden nie podaje jakichkolwlek szczegóÅ‚ów, a mówi ogólnikami, wiÄ™c wÅ‚aÅ›ciwie n
wiadaomo, jak temu przeciwdziaÅ‚aÄ‡, lub chociaÅ¼by utrudniaÄ‡ dla NSA zadanie.

Jedyne co pozostaÅ‚o na pocieszenie, to to, Å¼e USA na szczÄ™Å›cie nie sÄ… skore do wspóÅ‚ pracy z byle kim, wiÄ™c np p
sÅ‚uÅ¼by specjalne mogÄ… sobie conajwyÅ¼ej poprosiÄ‡ o rozkodowanie czegoÅ›tam i najczÄ™sciej dostaÄ‡ odpowiedÅº
odmownÄ… odnoÅ›nie dalszego przekazanie informacji.