

Rozdmuchane błędy w OpenSSL, klucz RSA złamany. I co z tego?

Wpisany przez Patryk yarpo Jar
niedziela, 14 marca 2010 04:46

Przez kilka ostatnich dni w miejscach poświęconych bezpieczeństwu huczało głównie na tematy związane z OpenSSL-em i łamaniem kluczy RSA. Ekipa Niebezpiecznika podchodzi do tych "rewelacji" z dużym dystansem, oto dlaczego: O co kaman? Mądre głowy z Uniwersytetu w Michigan wykombinowały sposób na domyślenie się fragmentów klucza prywatnego. Metoda polega na celowym zaburzaniu źródła prądu w trakcie operacji [...]

[read full article](#)