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