



13 - 14 MAJ 2006 KRAKÓW

---

Zbigniew Gołębiowski, Filip Zagórski  
"Kleptografia"

Kleptografia to sposób wykradzenia informacji, najczęściej kluczy, w sposób bezpieczny dla atakującego z wykorzystaniem szyfrowanego kanału podprogowego. Ataki kleptograficzne na aplikacje wykorzystujące protokoły kryptograficzne stanowią szczególnie niebezpieczną klasę zagrożeń. Wynika to z faktu, iż zmiany wprowadzone w aplikacji zachowują jej zgodność z protokołem.

Tym samym, ataki tego typu są trudne do wykrycia.

Zaprezentowane zostaną ataki na protokoły SSL/TLS i SSH, scenariusze ich przeprowadzenia, a także propozycje poprawek eliminujących zagrożenie.