

JUTARNJI LIST 26.02.2005

Matematičkim napadom do PIN-a u 15 pokušaja

Mike Bond i Piotr Zelinski, znanstvenici sa sveučilišta u Cambridgeu, objavili su rezultate istraživanja po kojem je moguće otkriti nečiji PIN (Personal Identification Number), broj bankomatske kartice, u samo 15 pokušaja. Radi se o složenoj matematičkoj metodi usmjerenoj na decimalne tablice pomoću kojih se u bankomatskom hardveru decimalni PIN pretvara u heksadecimalni broj.

Tehnika opisana u njihovom radu, koji se može pronaći na

<http://www.cl.cam.ac.uk/TechReports/UCA-M-CL-TR-560.pdf>, zabrinula je mnoge sigurnosne stručnjake. Dosad se mislilo da četveroznamenasti PIN nije moguće "provaliti" u manje od prosječno 5000 pokušaja. Ovom tehnikom mogu se, kako se u radu spominje, koristiti pokvareni bankovni namještenici i drugi "insideri" ne bi li dobili nečiji PIN u prosječno 24, a najmanje 15 pokušaja. Iako se i dalje radi o pogađanju, na taj je način moguće predvidjeti koje znamenke vjerojatnije mogu biti dio PIN-a. Autori rada predlažu da se uspoređivanje decimalnih i heksadecimalnih brojeva unutar bankomatskih hardverskih modula zamijeni sigurnijim i robusnijim sustavima.

M. Mataija