SLOVAR UPORABLJENIH POJMOV

Algoritmični nadzor: analize podatkov s pomočjo kompleksnih algoritmov, ki omogočajo avtomatsko razpoznavo in sledenje.

Analiza električne aktivnosti (ang. *Differential Power Analysis*): ena izmed *tempest tehnik*, ki na podlagi električne porabe omogoča napadalcu razkritje šifrirnih ključev.

Biometrija: proces zbiranja, procesiranja in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije.

Brezžična lokalna omrežja (ang. *wireless LAN network*): omrežja za brezžično povezovanje računalnikov. Navadno temeljijo na protokolu 802.11b.

Brisanje začasnega pomnilnika (ang. *swap file*): ob zaustavitvi računalnika na disku ostane vsebina začasnega pomnilnika, njegovo brisanje pa onemogoča poznejšo obnovitev vsebine pomnilnika, kakršna je bila ob izklopu računalnika.

CCTV (*Closed Circuit Television*): nadzorne videokamere.

Carnivore: računalniški program, ki ga ameriški državni organi uporabljajo za prestrezanje vsega uporabnikovega internetnega prometa. Uradno se sistem imenuje DCS1000. V ZDA deluje od junija 2000.

Cult of the Dead Cow: hekerska skupina, ki je leta 1998 na svoji spletni strani objavila trojanskega konja Back Orifice, ki je namenjen nadzorovanju računalnikov prek interneta.

Časovni napad (ang. *Timing Attack*): ena izmed *tempest tehnik*, ki na podlagi merjenja časa, ki ga naprava porabi za procesiranje, napadalcu omogoča razkritje šifrirnih ključev.

Čistopis (ang. *cleartext, plaintext*): osnovno, nešifrirano sporočilo.

Datoteka aktivnosti (ang. *log file*): datoteka, kamor se beležijo dejavnosti uporabnika interneta. Vzdržujejo jih ponudniki dostopa do interneta in ponudniki različnih storitev interneta (predvsem spletnih strani).

DES (*Data Encription Standard*): eden najbolj razširjenih kodirnih algoritmov, ki se je uporabljal v civilni sferi, predvsem v bančništvu. Ameriška vojska pozna bližnjico za njegovo razbijanje.

Distribuirano procesiranje podatkov prek interneta: procesiranje podatkov v omrežju računalnikov, povezanih prek interneta, kjer vsak računalnik sprocesira le košček informacije. Skupna procesorska moč tako povezanih računalnikov je zelo velika.

DNS (*Domain Name System*): sistem, ki skrbi za pretvorbo imen domen v ustrezne IP naslove. Zasnovali so ga leta 1983 na Univerzi Wisconsin v ZDA.

Družba dosjejev: družba, v kateri o vsakem posamezniku obstaja neki zapis, neki dosje. Ljudje tako čedalje bolj postajamo svoji dosjeji, saj ti tvorijo našo podobo.

Družba nadzora: družba, v kateri je nadzor maksimiran. Webster je namesto uporabe pojma informacijska družba predlagal uporabo pojma družba nadzora.

ECHELON: sistem, ki je bil prvotno zgrajen za prestrezanje komunikacij Sovjetske zveze, Kitajske in drugih držav, danes pa se uporablja tudi za prestrezanje civilnih komunikacij.

Elektronska sled: informacija, ki se shranjuje rutinsko in kaže na akcije določenega posameznika, tudi informacija, ki jo posamezniki za seboj puščamo v virtualnem prostoru.

Enkratno geslo (ang. *one-time password*): geslo, ki je uporabno samo za enkraten vstop v sistem.

Faktorizacija: poseben matematični postopek iskanja praštevilčnih faktorjev danega števila. Napadalec, ki bi mu uspela faktorizacija, bi lahko na podlagi tega postopka odkril zasebni ključ in tako dešifriral sporočilo.

GIS baze: podatkovne baze geografskih informacijskih sistemov. Z njimi se lahko poveže druge baze podatkov in satelitske posnetke.

Groba sila, napad z grobo silo (ang. *brute force attack*): preskušanje vseh možnih kombinacij gesel. Metoda grobe sile zahteva veliko procesorskega časa in je zato razmeroma neučinkovita.

GUID, globalni univerzalni identifikator (ang. *Global Unique Identifier*): identifikacijska številka, ki se zabeleži v vse dokumente programskega paketa *Microsoft* v *Office 97*, kar omogoča poznejšo identifikacijo avtorja dokumenta.