

# Statisztikai spamszűrők

---

Hatékony megoldás a spam ellen

Sütő János, [sj@acts.hu](mailto:sj@acts.hu)

# Az ideális spamszűrő

---

100% pontosság

Nagy teljesítmény

Telepítés 1 kattintással

Színes-szagos riportok

Ingyen elérhető

---

# Miért a statisztikai szűrők?

---

Nagy pontosság: >99.5%

A levél tartalmát vizsgálja

Megtanulja milyen a jó/rossz levél

Felhasználók bevonása

---

# clapf

---

E-mail tartalomszűrő alkalmazás

Nyílt forrású: zlib/png licence

Nem veszít el levelet

---

# Rugalmas konfiguráció

---

Postfix: after-queue content filter

(anti-spam gateway is)

.forward + maildrop

Virtuális felhasználók

Elosztott környezetben is

---

# Hogyan működik?

---

Levél dekódolása:

Base64

QP

UTF-8

URL

HTML

---

# Hogyan működik? (2)

---

Tokenekre bontás:

From\*norio Subject\*impress lover sexual

Subject\*yourpartner increase blow

longerOrgasms enhanced+libido

doubles triples absolutely

# Hogyan működik? (3)

---

Tokenek valószínűségének kiszámítása:

$$p(h) = N_{ham}/N_{HAM}$$

$$p(s) = N_{spam}/N_{SPAM}$$

$$p(w) = p(s) / (p(h) + p(s))$$

# Hogyan működik? (4)

---

Döntési mátrix (~15 token):

enhaced+libido 0.9999

blow 0.9999

sexual 0.9251

absolutely 0.9000

---

# Hogyan működik? (5)

---

Statisztikai összegzés:

Bayes-i (dspam)

Inverz khi( $\chi$ ) négyzet (bogofilter)

Markov lánc (crm114)

...

# Hogyan működik? (6)

---

$$P = (1-p_1) * (1-p_2) * \dots * (1-p_n)$$

$$Q = p_1 * p_2 * \dots * p_n$$

$$H = \text{chi2inv}(-2 * \ln Q, 2*n)$$

$$S = \text{chi2inv}(-2 * \ln P, 2*n)$$

$$I = (1 + H - S) / 2$$

---

# Token adatbázis

---

MySQL: rugalmas, kényelmes

SQLite: 1 fájl, nagyon gyors

Qcache: token gyorsítótár, ~5 MB RAM

# Token adatbázis (2)

---

közös (shared):  $uid=0$

összegyűrt (merged):  $uid=0 + uid=x$

levél: nekem ham + neked spam

610(200)k token (8k ham, 10k spam)

numerikus tokenek ( $2^{64}$ )

---

# Token adatbázis tanítása

---

Automatikus tanulás ( $n < 1000$ )

Hiba esetén (TOE)

Új adat esetén (TUM)

A spammerek is segíthetnek!

# Token adatbázis tanítása (2)

---

Gyártófüggetlen adatbázis

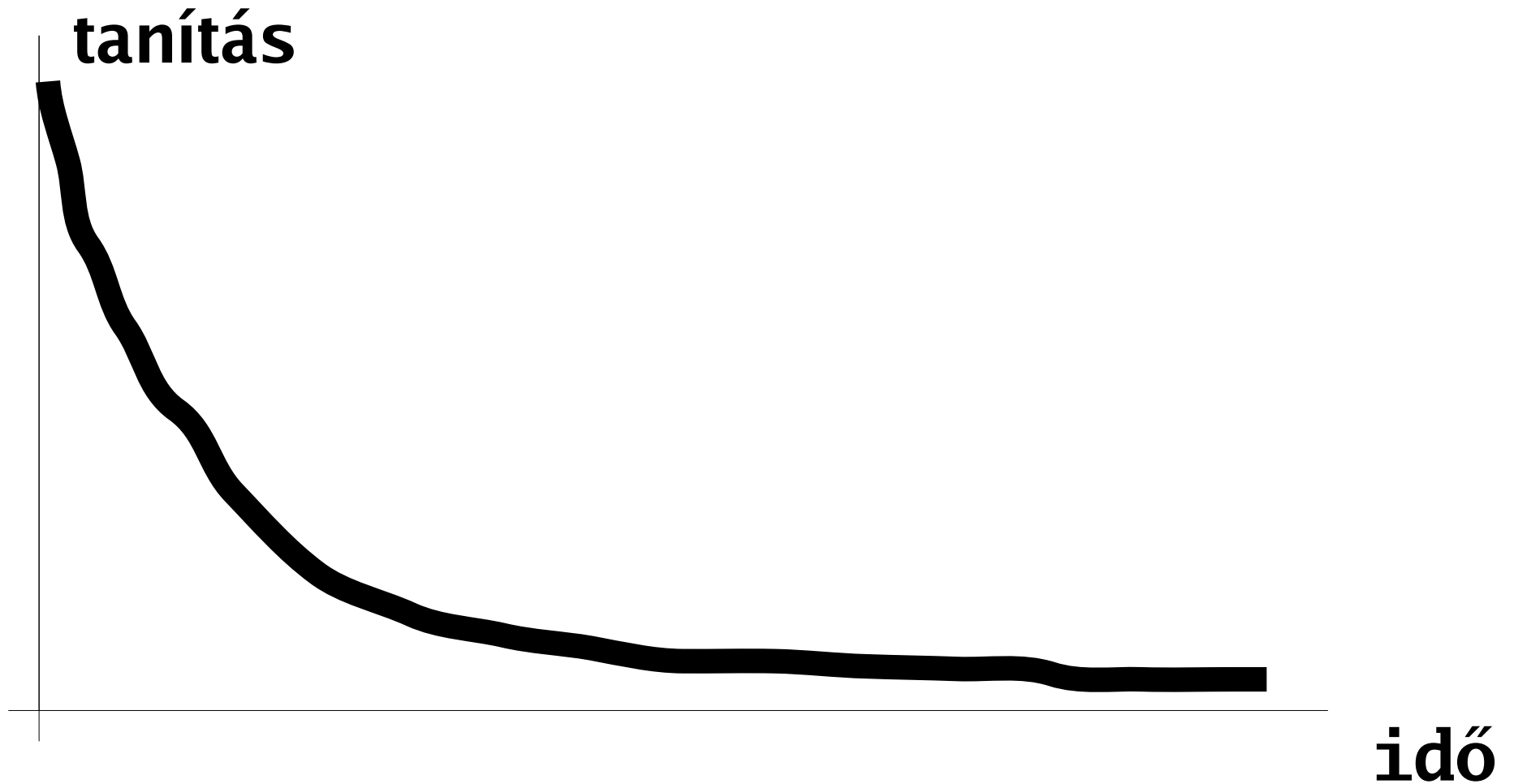
cmdline: adminisztrátor + shell users

web oldal: 1-2 kattintással

forward: bela+spam@xxxx.hu

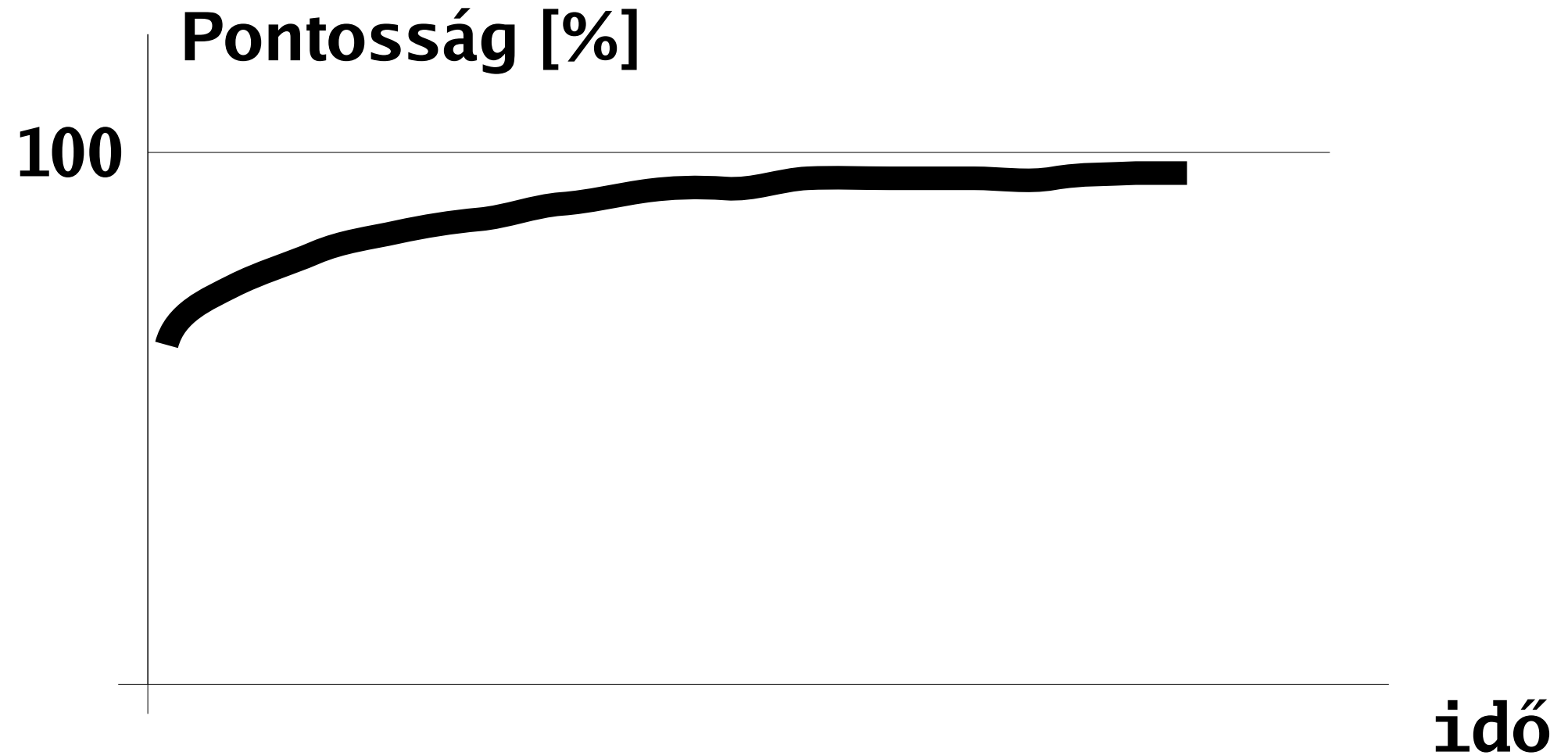
# Token adatbázis tanítása (3)

---



# Token adatbázis tanítása (4)

---



# Aknamező (blackhole)

---

Intelligens feketelista

Csapda e-mail cím hirdetése

Küldő IP-címe könyvtárban tárolva

Előregedett címek törlése (cron)

~2k levél/hónap

---

# Feketelista

---

Ha nem elég jó a levél (>0.41)

URL-ek + kliens IP-cím ellenőrzése

Nyilvános listák: URIBL, SURBL, CBL

Saját lista: rbl.xxxx.hu

Sebesség?

---

# Image spamek

---

OCR? (hatásfok, erőforrás igény)

Speciális token: IMAGE\*, EMBED\*

Ha nem elég jó a levél (>0.41)

Döntő többségét felismeri

PDF, RTF, ... spam ellen is

---

# Idegen nyelv felismerés

---

Ha nem elég jó a levél ( $>0.41$ )

Ismeretlen (érthetetlen) karakterek

Koreai, orosz, portugál, ...

Ha a számuk elér egy limitet

Karakterkonvertálás: jjj jj jjjj j

---

# Spam karantén

---

Felhasználónkénti karantén

Megnéz, töröl, tanít, továbbít

Böngészőből elérhető

Régi spam automatikus törlése (cron)

---

# Felhasználói preferenciák

---

LDAP vagy SQL adatbázisban tárolva

Spam karantén beállítások

Mit tegyünk a spammal?

megjelöl | karantén | eldob

# Támadások

---

Szó saláta vagy véletlen szöveg

Kreatív írás (V1agara, Order n0w!)

Félbevágott szavak (Curre nt p+rice)

Szükségtelen kódolás (base64, HTML)

Melléklet spamok (jpeg, pdf, xls)

Bayes-i mérgezés

Micro/pico spam

---

# Hiedelmek

---

„A token adatbázist folyamatosan tanítani kell”

„A spam szavak egyediek a felhasználóra nézve, nincs globális ham/spam táblázat”

---

# Hiedelmek (2)

---

Magyar sajátosságok

„Szélsőségesen tanított” szűrő

A spammerek védekeznek ellene

Több GB a token adatbázis

# Számok

---

Átlagos kategorizálási idő: <200 ms

Rekord:  $1008/1009=99.9\%$  (15 nap)

Spam rekord:  $642/643=99.84\%$  (10 nap)

# Mindjárt vége . . .

---

Clapf: <http://clapf.acts.hu/>

Blog: <http://sj.acts.hu/>

# **Köszönöm a figyelmet!**

---

Kérdések?