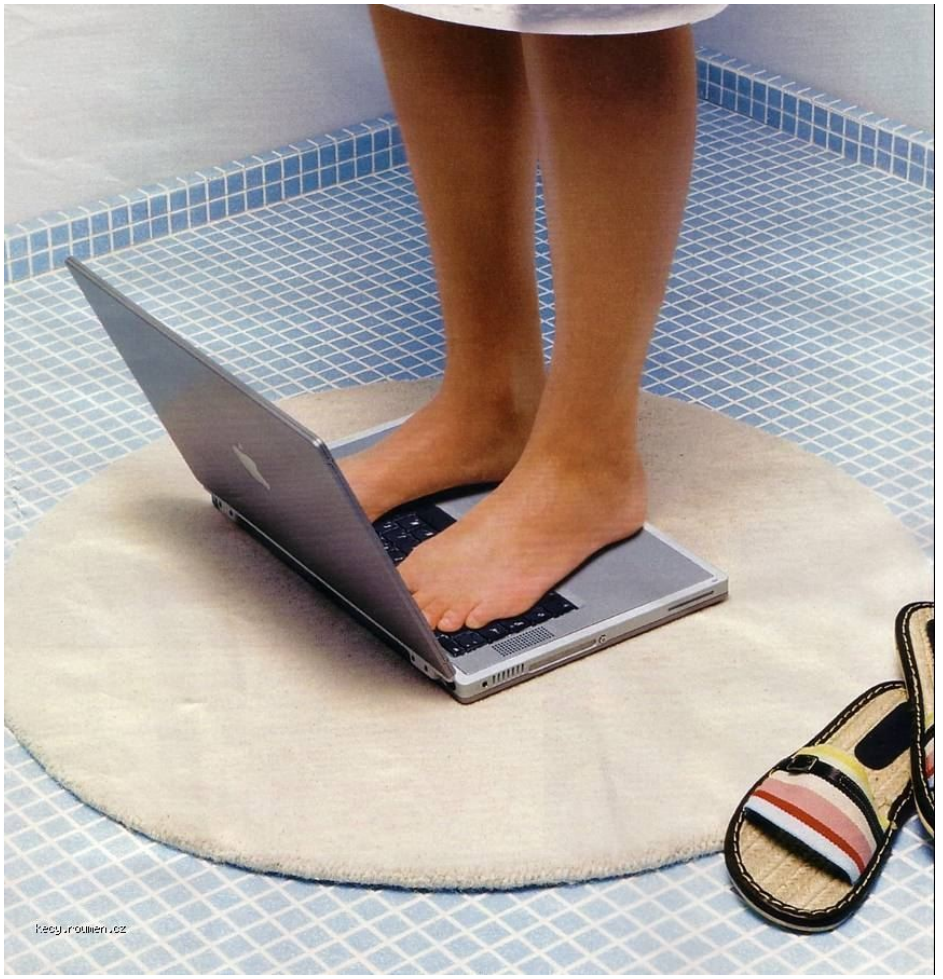
R&D @ CZ.NIC

CZ.NIC z.s.p.o.
Ondřej Surý
ondrej.sury@nic.cz
May 09 2009

cz nic
cz domain registry

CZ.NIC Labs

- Approved IV.Q 2008
- Started I.Q-II.Q 2009
- Team of 4-5 people
  - Full time
  - Part-time (grad students)



Mission

- Service for public interest
- Focus on local (Czech) internet community
- Strong separation from operations
- Cooperation with other subjects:
  - DNS OARC, IETF, NLnet Labs

Research

- Technologies
  - DNSSEC
  - IPv6
- Security
  - Honeynet
- DNS Monitoring

Development

- DNSSEC
  - DNSSEC in Debian
  - Tools
- The BIRD Internet Routing Daemon
  - http://bird.network.cz/

Education

- Lectures on DNS, DNSSEC, ENUM, BGP
  - Open to general public
  - Vendor independent
- Opponent for D.I.P. competition
  - Sort of Summer of Code program
- Cooperation with universities
- Articles in technical magazines
- Book publishing / writing

Results

- Software under open source licenses
- Full tech reports published in Czech
  - Englisch translation on best effort basis

Running and New Projects

- Work in Progress
- Just started
- Mainly ideas to discuss

Antispam

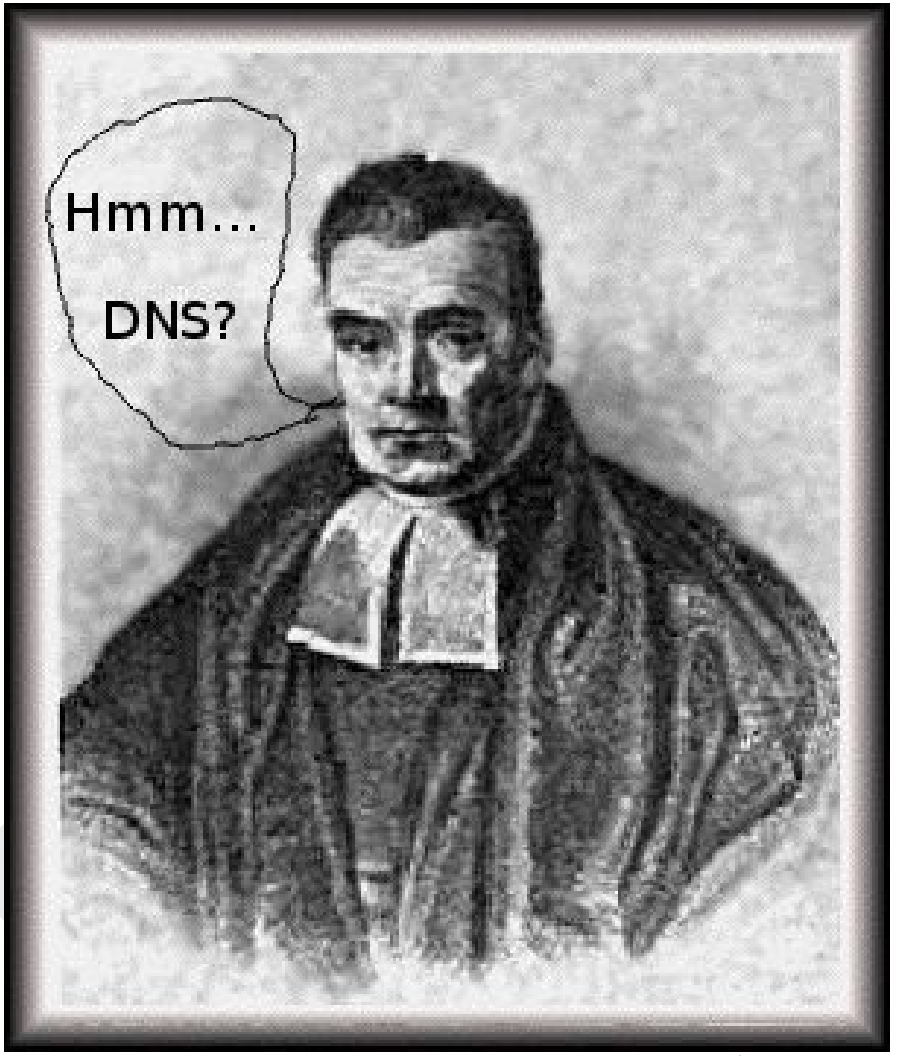
- Short analysis
- Current techniques
- What can be done?
- Content classification
  - So effective
  - Stopped innovation

DNSSEC SOHO/CPE test in CZ

- In-house test
  - Bought equipment "in the wild"
- Downloadable client
  - Written in Python
  - Submissions reviewed by person
  - Report online on web
- Everybody is welcome to join

Bayesian classification of DNS

- Tokenize DNS traffic
- Classify it:
  - SpamBayes, CRM114, ???
- Possible usages
  - Resolver side – detect zombies, wrongdoers
  - Authoritative side – analyze strange traffic (?)



CUDA DNSSEC signer

- CUDA technology
- Many cores on GPU
- Fast DNSSEC signer

- nVidia Tesla Card →
  - 240 cores

TLSFP RR Type

- Similar to SSHFP RR Type
- For SSL/TLS connections
- Intended to help where self-signed cert is OK
  - Intranets/Mail servers/Home use/etc.
- Not-intended to replace CA
- I-D on its way
- Discussion in IETF dnsext (namedroppers)

Questions?

Ultimate problem