Autonomica

Robust Drift av Rotnamnservrar

Lars-Johan Liman
Autonomica AB

Autonomica

Rotnamnservrar – vad är det?

- Ingången till DNS-systemets databas.
- Rotnamnservrar kan alltid leda vidare in i systemet, eller tala om att något inte existerar.

Autonomica

MÅNGA frågor

- Stockholm: c:a 4.000 frågor/sekund.
- .... vilket motsvarar 345.600.000 frågor/dag.
- a.root-servers.net brukar ligga på 14.000 frågor/sekund.

Autonomica

DUMMA frågor

- 8-10% kommer från nät 10.0.0.0/8 (privata) etc.
  - Vi kan inte svara. Filtreras bort.
- 3,6 % frågor **OM** net 10.in-addr.arpa, 168.192.in-addr.arpa.
  - Detta trots att vi har delegerat ut dem ...
- 4% frågar om "localhost".
  - C:a 13.720.000 frågor/dag.
- 3% frågar om toppdomänen ".local".
- 2,3% rekursiva frågor.

Autonomica

DUMMA frågor

- Slafsigt uppsatta system

  `_ldap._tcp.Standardname-des-ersten-Standorts._sites.gc._msdcs.USD.local`

- Marjasinproblem

  `SC1DREV_TByggesagerIgangv\145rende\032sagerSag\032011.09\032Ny\032receptionsskranke\032afsnit\0323981Rekvisition_J\032Pihl.doc`

Autonomica

Försvar?

- Nej, egentligen inte.
- Information och utbildning.
- Lev och lid.
- ".local" speciell.
  - Politiskt problem som kan bli prejudikat, om inte hanteras försiktigt.

Autonomica

Buggar i kod.

1. Säkerhetshål i DNS-koden?
   - Mycket nära kontakt med de som skriver koden.
2. Säkerhetshål i operativsystem?
   - Kända system med öppen kod och många användare.
3. Såkerhetshål i routrarnas operativsystem?
   - God relation till tillveraren.

Autonomica

Attacker

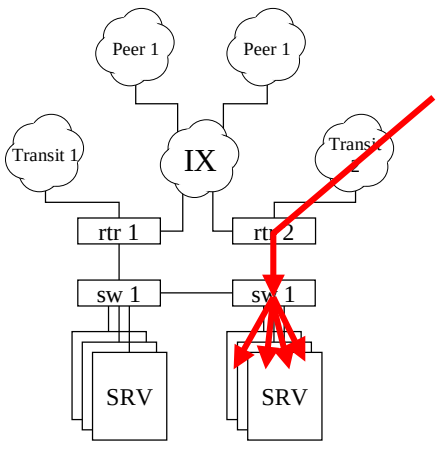
- Avsiktligt "trasiga" frågor som försöker hitta och/eller utnyttja säkerhetshål.
- Cache pollution?
  - SEP.
- Distributed Denial of Service Attacks.
  - We don't lik'em. ☹
  - Vi får dem så ofta att de flesta bara är brus.

Autonomica

Lastdelning

- Frågorna sprids mellan flera servrar i samma installation.
- Nästan alla rötter gör detta i dagsläget.

Autonomica



Autonomica

Lastdelning

- Bra idé.
  - Ökar frågekapaciteten.
  - Skalar linjärt.
- men ...
- Nätets periferi är alltid större än varje givet serverkluster.

Autonomica

Anycast

Vad är anycast?

- Ett sätt att installera fler servrar på fler ställen.

Varför anycast?

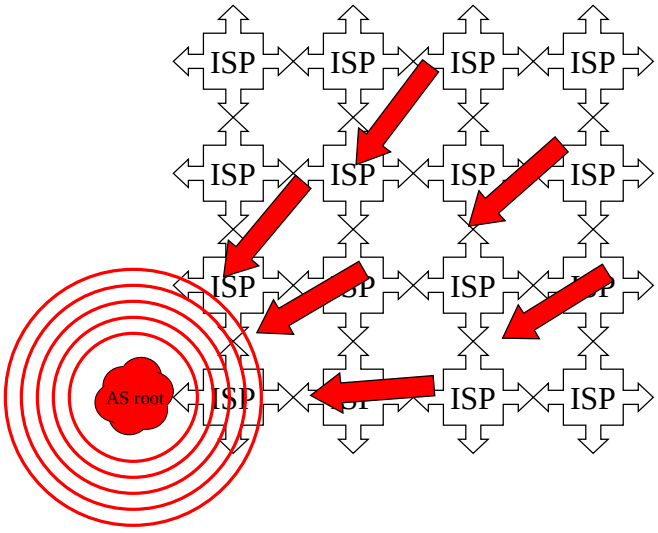
- Bättre tjänst till fler användare.
  - Ingen har lyckats bestämma om ***var*** man skall ställa nya rötter. Root-ops gör själva.
- Dämpar effekterna av DDoS-attacker.

Autonomica

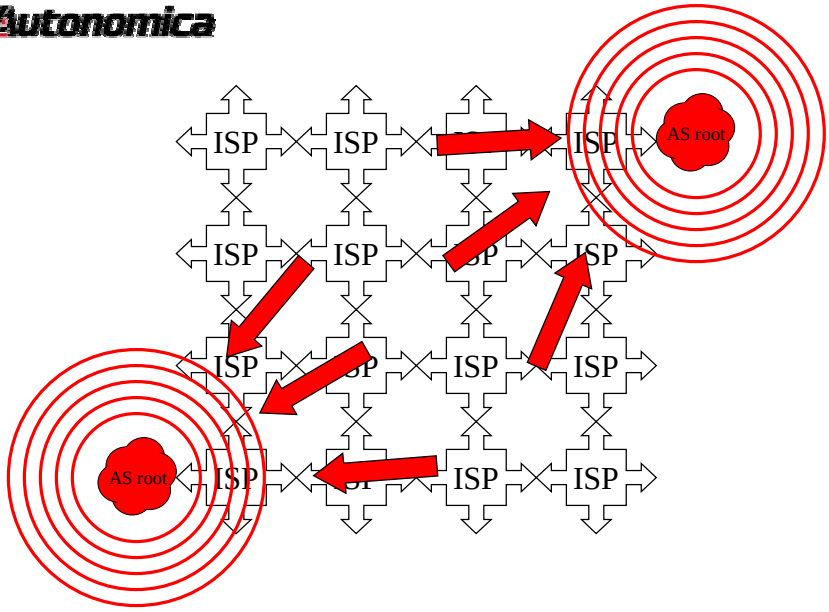
Hur funkar anycast?

- Servrar på flera ställen på klotet.
- ***SAMMA*** nätverksinformation.
- ***SAMMA*** data.
- ***OLIKA*** servrar.
- Routingsystemet bestämmer vart klientens fråga skall skickas.

Autonomica



Autonomica



Autonomica

Fördelar med anycast.

- Tjänsten närmare konsumenterna.
- Automatisk lastdelning.
  - Stora talens lag ...
- Automatisk fail-over.
- Lokalisering av attackscenarier.

MYCKET VIKTIGT!

Autonomica

Nackdelar med anycast?

- Rubbar jämvikten.
- Komplext.
  - Bryter mot kända principer (KIS, PLS, 1-to-1).
- Svårt att administrera.
  - Övervakning.
  - Åtkomlighet.
  - Dataöverföringar.
- Svårt att felsöka.

Autonomica

Dagsläget?

- 7 av 12 rootserveroperatörer gör det i någon form. Några ex:
  - M: servarar i Tokyo och Osaka sedan 1998.
  - I: Stockholm, Helsingfors, (Milano), (London)
  - F: Ottawa, Palo Alto, San José, New York, San Francisco, Madrid, Hong Kong, Los Angeles, Rom, Auckland, São Paulo, Seoul, Johannesburg
  - K: London, Amsterdam, (Wien)
  - C: Gör lite annorlunda. Endast inom eget nät.