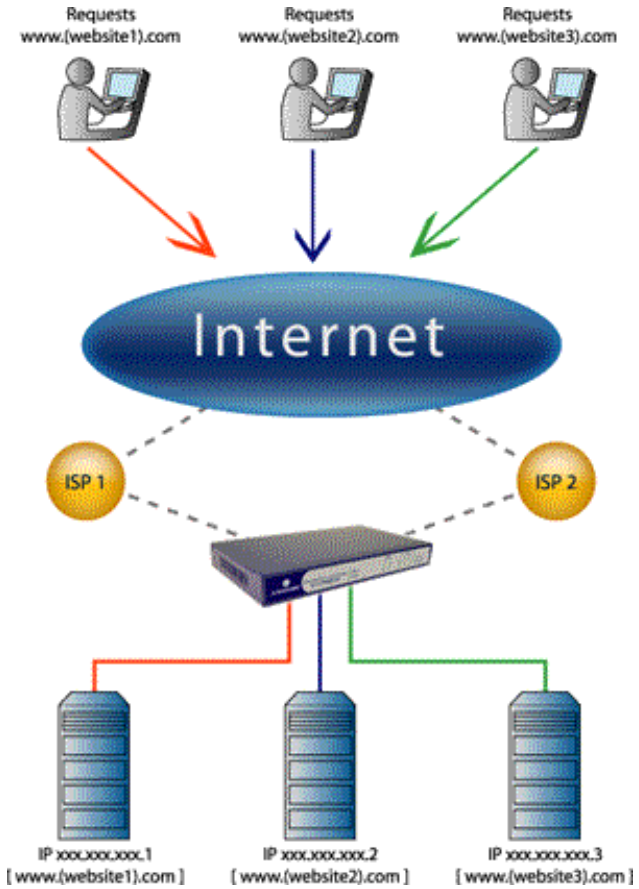
DNSSEC

Petr Baudiš ⟨pasky@ucw.cz⟩

brmlab lightning talks 2012-01

DNS

- **Domain Name System:** translate human-friendly names to internet addresses
- In fact a general distributed directory service
- Caching recursive nameservers and zone hierarchy
- Scalable distributed system, no security in mind



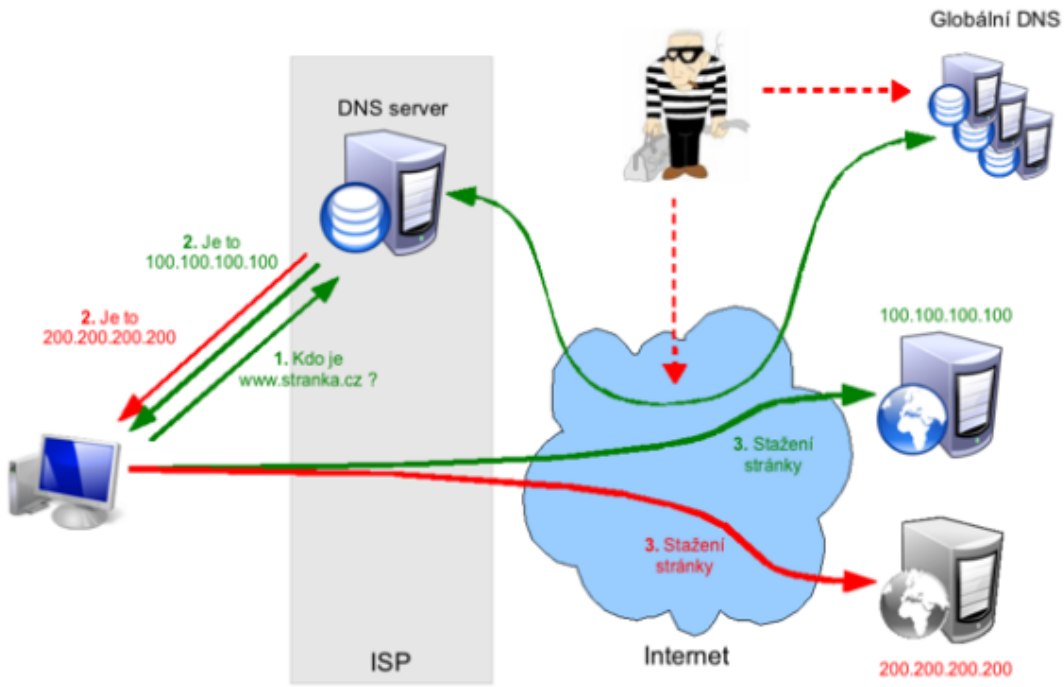
DNS: Security Issues

Fake replies:

- `google.com. IN A 77.87.241.77`
- `google.com. not found`

Easy to generate:

- Compromising nameserver
- Intercepting traffic
- Cache poisoning



CZ.NIC

Other issues (less interesting)

- False assumptions about name ownership
- Confidentiality of data
- Denial of service

Solution: DNSSEC

Prevent fake replies.
Keep backwards compatibility.
Protocol enhancements — extra records and reply bits.

- Public key cryptography
- DNS replies are cryptographically signed
- Hierarchy of trust: chain of certificates
- Trusted third party (anchor): Root zone
- Key Signing Keys and Zone Signing Keys
- DO, CD, AD packet bits
- RRSIG: signature of resource record
- DNSKEY, DS: pointers to certificates
- NSEC, NSEC3: proof of non-existance

DNSSEC adoption

Domains

- CZ.NIC: Adoption leader (cz); Web4U
- Other examples: `br`, `bf`, `pr` or `se`
- Reverse zones: Signed
- Root zone: Signed!

Clients

- Typically, recursive nameserver performs validation
- Limited support for otherwise

Thanks

Petr Baudiš ⟨pasky@ucw.cz⟩