PowerDNSSEC: A different way of doing authoritive DNSSEC

Bert Hubert
PowerDNS.COM / Netherlabs Computer Consulting

POWERDNS

Agenda

- PowerDNS “The Company”
  - 100% open source, 100% carrier grade
- PowerDNS “The Software”
- PowerDNSSEC Profile
- PowerDNSSEC Technical Details
- PowerDNSSEC Roadmap

PowerDNS: The Company

- PowerDNS, 100% open source DNS technologies, 100% carrier grade, around since 1999
- Provides software, training, support, consultancy, professional services
- Rolver customers include many “Flag Carriers” - many of them represented in this room
  - “X Telecom”, “Royal Y Telecom” etc
- Powers 40+% of all .NL domains, 50+% of all .DE domains, server of choice for very large auth deployments
- Main business model: create great software that can be supported 24/7 – because it works

PowerDNS: The Software

- Authoritative Server: Serve DNS at high speed from Oracle, Sybase, DB2, Microsoft SQL Server, MySQL, PostgreSQL, DB2, LDAP, SQLITE2/3, Perl/Python/C++ backends, Geograpical Loadbalancing data and even.. plain zonefiles ('BIND mode')
- Resolver: “rock solid, carrier grade DNS resolution”, with powerful scripting abilities
- Tooling: validate DNS performance in various ways
  - “Vendor assurance”

PowerDNSSEC Profile

- Large installed PowerDNS Userbase
  - Need to do DNSSEC (one day)
- We still like the PowerDNS Philisophy
  - “Just update the database, and things work”
- After lots of discussions and consultations, it was decided to do “PowerDNSSEC” in a similar way
  - Very different from existing setups
- The goal: provide DNSSEC in a way that does not require new personnel
  - But perhaps an additional server
- Secondary goal, be 'compliant & ok' out of the box

PowerDNSSEC

- All the things you need: NSEC, NSEC3, SHA1, SHA256..
- Operates based on unsigned, “plain old DNS” data
- Database format is almost unchanged, there is now an additional 'ordering' field
  - For NSEC/NSEC3
- Signing is online & heavily cached
- Signatures auto-rotate, keys do not
  - ZSK rolls over on demand

“PowerDNSSEC” differences

- Live signing!
- Keying material partially **on** the server
  - KSK can be separate
- Database based, even support scripts for dynamic DNSSEC
- Less room to tinker than manual signing, less room to make mistakes
- Serves .NET zone at 30000qps from scratch
  - Once all signatures are cached, normal >100kqps performance
- Aimed at places that do not necessarily love DNSSEC

PowerDNSSEC: Status

- Part of PowerDNS Authoritative Server 3.0 prereleases
  - Full release expected Real Soon Now
  - Various very large hosters ready to be the launching customer
- Resolver will follow

Questions?

- Questions?
  - Here & now
- Otherwise: bert.hubert@netherlabs.nl
- “E164”: +31-6-22440095