DNSSEC
Basics

Peter Koch
DENIC eG
pk@DENIC.DE

Luxembourg, 2005-07-12

Agenda

- Why? – DNS weaknesses
- Why, really? – . . . and when they matter
- What can implementations do?
- What will DNSSEC achieve?
- How does it work?

DNS Weatures

- Millions of Interacting Components
- No Cryptographic Security
- Lightweight, UDP based

  No *Connections*
- 16bit ID space

  Guessing, Flooding, *Birthday* Attacks
- Caching, Additional Section Processing

  Kashpureff Style Attacks

Today's Implementations

- Ignore much *Additional Information*
- Apply Credibility Heuristics to DNS Answers
- Truly Randomize IDs and Ports
- Allow for Restricted Recursion
- are Strengthened but Not Immune

The Main DNSSEC Benefits

- Data Origin Authentication
  - Data Forgery will be detected
- Data Integrity
  - Data Modification will be detected

How are the Benefits Achieved?

- Industrial Grade Public Key Signatures
- No PKI needed, leverages on DNS Scalability and Pervasion
- Vendor Independent Technology (IETF Proposed Standard)
  (RFCs 4033, 4034, 4035, March 2005)
- Per Zone Key Pair
- Chain of Trust through the well known Delegation Process

Some DNSSEC Details

- Authenticates DNS Resource Record Sets
  (*All addresses of* `www.example.org`)
- . . . as well as the Absence of Records or Names
  (`rss.example.org` *does not exist*)
- Introduces four New DNS Record Types
- Full RFC 4033-35 support in BIND 9.3 and NSD 2

Almost Gory Details

- Zone Maintainer generates per Zone Key Pair
- Public Key is Published through DNS
- Private Key is used to sign . . .
  - all Records
  - all Gaps between Names
  - DS Records for Delegated Child Zones
- Signatures are *piggy backed* on DNS responses
- . . . if querying client signaled DNSSEC capability

Registries' Tasks

- Have DNSSEC Capable Name Servers for the TLD
- Have Policies in Place
- Registrar Interaction
- Key Handling
- Signatures over DS Records

The main DNSSEC costs

	End User	Domain Holder	ISP	Registrar	Registry
CPU cycles	X		X		X
Key Management	(X)	(X)	X	(X)	(X)
Expertise			X	X	X

Is DNSSEC Really Necessary?

- We do not fuel panic, there's no guarantee for attack tomorrow
- . . . However, spoofing tools are readily available
- Most target the local recursive server
- . . . but some are more sophisticated
- Even sophisticated implementations with enough random cannot protect against spoofing
- This is not only about bugs, it is about a protocol inherent vulnerability
- There are too many components that need to be configured correctly
- Currently, the incentive is low
- . . . since, e.g. phishing is much easier

Where DNSSEC fits

- DNSSEC is not a panacea
- . . . but a Piece of the Security Puzzle
- You know, we have Safety Belts and Airbags and ESP and Guard Rails and . . .
- `https` is Not Enough
- . . . and Not Always Applicable

Time to Say *Hello*

- DNSSEC needs preparation
- Can’t just *Ship a Patch*
- Needs Interaction with Registrars and/or Customers (DNS Zone Maintainers)
- So, when attacks start next year, you better start preparing today

Why we, why now?

- Honestly, we are trying to be responsible
- Initiative for security measures has always come from the outside
- Ban of cleartext passwords (in protocols) needed a strong word from the IESG
- Secure DNS Tree needs Signed TLDs (and Root!)
- Helps Securing the Underlying Technical Infrastructure