DNSSEC Practicum Assignments
DNS Security Extensions

N.P.H. Sijm
niels.sijm@os3.nl

14 September 2012

Abstract

In the practicum, you will set up a DNSSEC-validating DNS resolver, use DNSSEC to secure your own zone and delegate a zone to one of the other students.

1 Introduction

DNS has been designed without security in mind. Since security researcher Dan Kaminsky demonstrated the ease of DNS cache poisoning, DNSSEC, a DNS security extension, has become popular. DNSSEC is an open standard, documented in various RFCs, that adds cryptographic protection to DNS making it hard to forge DNS replies.

Before the DNS root servers and the Dutch ccTLD got signed, people had to work with "islands of trust". Nowadays, we can use DNSSEC by having to know just the DNSSEC keys of the root servers. If you are interested in legacy DNSSEC operation, "islands of trust" are nice to experiment with.

2 Setting up a validating resolver

In order to get familiar with DNSSEC, we first set up a DNSSEC-validating resolver. You can use the BIND installation from the previous practicum.

1. Add support for DNSSEC to your BIND configuration. What changes do you have to make to your configuration?

Since the DNS root servers have been signed, "native" DNSSEC validation is possible for some domains. Use `dig` to verify the validity of DNS records for `isc.org` and `os3.nl`.

2. How does `dig` report on the DNSSEC validation results?

The only way to really test your resolver is by breaking the chain of trust. In more recent versions of BIND, this is not as simple as you would think it is.

3. Where does BIND store the DNSSEC root key?

4. How do "managed keys" differ from "trusted keys"?

Modify the DNSSEC root key of your BIND installation and try to validate the chain of trust again.

5. How did you modify the DNSSEC root key?

6. What problems did BIND encounter, and how did BIND react?

3 Setting up a secure zone

Adding DNSSEC to an authoritative nameserver is a delicate process. First one has to decide upon the chain of trust: does the parent zone offer secure delegation, or do I create an "island of security"? Cryptographic algorithms, key sizes, key lifetimes and key rollover schemes have to be chosen, generated and configured.

7. Look up which cryptographic algorithms are available for use in DNSSEC. Which one do you prefer, and why?

Although the specification does not require it, all major DNSSEC tools use two different kind of keys: a key-signing key (KSK) and a zone-signing key (ZSK). When a ZSK changes, the parent zone is not involved. When the KSK changes, the parent zone needs to be involved in order to maintain the chain of trust.

8. In practice, different algorithms, key sizes and key lifetimes are chosen for KSKs and ZSKs. Discuss these differences and their motivation.

9. Choose appropriate algorithms, key sizes and key lifetimes for your KSK and ZSK.

There are various tools that can generate keys and sign zones. In this practicum, we are using the BIND9 tools. Use `dnssec-keygen` to generate the KSK and ZSK for your zone and `dnssec-signzone` to sign your `<city>.practicum.os3.nl` zone.

10. Take a look at the signed version of your zone file. Does it look as expected?

Edit the BIND configuration to include the signed version of your zone file. Restart BIND and look at the syslog for errors. If BIND appears to be up and running, test DNSSEC by querying your server for the DNSKEY of `<city>.practicum.os3.nl`.

In order to create a chain of trust, you have to make your DS records known by Niels, the OS3 system administrator. Publish the DS records on your wiki and send Niels an email with your DS records *and* a link to the corresponding wiki page. Because the wiki is accessible over SSL only and you are authenticated by the wiki system, this is considered secure enough for this practicum.

4 Delegating a secure zone

Now you are familiar with DNSSEC zone administration, you can delegate zones within your own zone. Select one of your fellow students as your DNSSEC buddy and negotiate a nice subdomain like `<foo>.<city>.practicum.os3.nl`.

Create a zone file containing one SOA record and some A records for your delegated subdomain. Create DNSSEC keys and sign your new zone.

Next, you have to send the DS records to your buddy. Think of a secure way to send your DS records to your DNSSEC buddy.

11. Integrity is important because you want your buddy to include the right DS records. Is confidentiality also an issue? Explain.

12. Exchange DS records with your buddy in a secure way.

Add the DS records of your buddy to your own zone. Do not forget to re-sign your zone and reload BIND!

13. Verify the integrity of your buddy's resource records using `dig`. Is the `ad` flag set?

5 Extra assignments

Because DNSSEC keys have a limited lifetime, key rollovers are part of DNSSEC.

14. Discuss the different rollover schemes and their implications.

15. How does a KSK rollover differ from a ZSK rollover?

16. Which scheme would you favor for your own zone?

NSEC is used to prove that a certain resource record does not exist. A nasty side effect of NSEC is that it enables zone traversal. Using NSEC3, a DNS server can prove the non-existence of a resource record without facilitating zone traversal.

17. What are the main differences between NSEC and NSEC3?
18. Does the root use NSEC or NSEC3? What about the `.org` domain?
19. How common is NSEC3? How do tools respond to it?