INF142 submission one.

By Kristian Os

October 17, 2016

1 DNSSEC

1.1 Definitions

- DNS - is an abbreviation for Domain Name System
- DNSSEC - for Domain Name System Security Extensions.
- Root zone - This is the first node the DNS looks in the DNS hierarchy
- ZSK - Composed of a public key and a private key. Used to sign the fields in the area[2]
- KSK - Composed of a public key and a private key. Used to sign the ZSK keys.[2]

1.2 What does DNS do?

To reach another node on the Internet there must be denoted a number/name as an address. It must be unique so that one address only can point to one node.
ICANN manages these so that each node has one of these unique addresses. For the same reason as we do not reference our devices based on their MAC-addresses, DNS translates the name version of the address to a number. This makes it much easier to remember the different number versions of the address.

1.3 Security

Within the DNS there are no security measures that can stand to the modern attacks that are getting more complex and malicious by the day. Recently a vulnerabilities in the DNS were found that allowed an attacker to redirect a DNS lookup to retrieve a false IP-address. This way the user gets a fake version of the intended site and the attacker can steal information or manipulate messages/transactions for their own gain.

1.3.1 vulnerability? (Before DNSSEC)

One DNS variant is DNS cache poisoning. For this exploit to work the attacker must get control of a DNS server and a DNS lookup must go through the poisoned DNS server. The attacker points an address like ”www.uib.no” to a malicious IP-address. This way when a user types in ”www.uib.no” he gets redirected to the malicious version of the site that the attacker owns.

1.3.2 After the implementation of DNSSEC

With the implementation of DNSSEC organisations like UIB, Google and even the big tech leaders that controls the big nodes can sign the DNS records using public-key cryptography[1] Now that each DNS server is signed with one of these keys the browsers know when a server is compromised and can select another one that is trusted.

Keys - KSK and ZSK KSK is a long term key and ZSK is a short term key. For the root zone these keys are generated at different intervals. These events are called "Root KSK Ceremonies" and here the KSK is used to sign a set of ZSKs that will be used to sign the DNS root zone for three months until the next new ceremony.‘ [3]

2 Two-factor authentication

2.1 Definition

References

[1] Dnssec what is it and why is it important? https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en. Accessed: 10.10.2016.

[2] How to set up a dedicated server dnssec zone. http://help.ovh.co.uk/dnssec#link2. accessed: 13.10.2016.

[3] Root ksk ceremonies. https://www.iana.org/dnssec/ceremonies. accessed: 13.10.2016.