### Assignment 9: DNSSEC

DNSSEC (DNS Security Extensions) is designed to prevent network attacks such as DNS record spoofing and cache poisoning. Generally, the DNSSEC server for example.com will posses the IP address of www.example.com. When queried about this record that it possesses, the DNSSEC server will return its answer with an associated signature. If the DNSEC server is queried about a host that does not exist, such as doesnotexist.example.com, the server uses NSEC or NSEC3 to show that the DNS server does *not* have an answer to the query.

Suppose a user R (a *resolver,* in DNS terminology) queries a DNSSEC *server* S, but all of the network traffic between R and S is visible to a*network attacker* N. The attacker N may read requests from R to S and may send packets to R that appear to originate from S.

1. Why is authenticated denial of existence necessary? To answer this question, assume that S sends the same unsigned DOES-NOT-EXIST response to any query for which it has no matching record. Describe a possible attack.
2. Assume now that S cryptographically signs its DOES-NOT-EXIST response, but the response does not say what query it is a response to. How is an attack still possible?
3. A DNSSEC server may send a signed NSEC response to a query that does not have a matching record (such as doesnotexist.example.com). An NSEC response contains two names, corresponding to the existent record on the server that immediately precedes the query (in lexicographic order), and the existent record that immediately follows the query. For example, if a DNSSEC server has records for a.example.com, b.example.com, and c.example.com, the NSEC response to a query for (non-existent) abc.example.com contains a.example.com and b.example.com because these come just before and just after the requested name. To be complete, NSEC records also wrap-around, so a query for a non-existent name after the last existent name will receive an NSEC containing the last and first existent names.

How should the resolver use the information contained in NSEC records to prevent the attacks you described in previous parts of this problem?

1. NSEC leaks information that may be useful to attackers on the Internet. Describe how an attacker can use NSEC to enumerate all of the hosts sharing a common domain-name suffix. How is this information useful for attackers?
2. NSEC3 is designed to prevent DNS responses from revealing unnecessary information. NSEC3 uses the lexicographic order of hashed records, instead of their unhashed order. In response to a query without a matching record, NSEC3 will return the hashed names that are just before and just after the hash of the query. For example, on a server containing a.example.com, b.example.com, and c.example.com, if a hashes to 30, b to 10, c to 20, and abc to 15, the NSEC3 response to a query for abc.example.com would contain 10.example.com and 20.example.com. Hashed names are also assumed to wrap around, in the same way as unhashed names in NSEC.

Explain how a resolver should verify the validity of a response under NSEC3?