CIA Lab Assignment:
DNS Security Extensions (DNSSec)
and DNS-over-HTTPS (DoH)

Task 1 - DNS Insecurity

- In what context was the DNS cache poisoning attack discovered? (Who, when, why)
- How does this attack work and how to prevent it?
- What is DNS spoofing and what tools can be used to integrate this attack?
- What does a validating resolver do? What is the difference between island-of-trust versus full-chain-of-trust?
- Does DoH substitute DNSSec or complement it? What are the differences between them?
- What do you think about DoH vs DoT vs DNSCrypt?

Task 2 - Validating Resolver

Setup

- Enable DNSSec to your BIND or Unbound and verify the root key is used as a trusted source.
- Use *dig* or *drill* to verify the validity of DNS records for *isc.org, sne21.ru*

Validate

- How does *dig* or *drill* show whether DNSSec full-chain-of-trust validation was successful or not? *Hint: it's about a flag*

Counter-validate (breaking the chain of trust)

- Where does BIND or Unbound store the DNSSec root key?
- How do managed keys differ from trusted keys? Which RFC describes the mechanisms for managed keys?
- Modify the DNSSec root key and test your validating resolver.
- How did your server react?

Task 3 - Secure Zone

Island of trust

- Look up which cryptographic algorithms are available for use in DNSSec. Which one do you prefer, and why?
- What is the difference between Key-Signing Key (KSK) and Zone-Signing Key (ZSK)?
- Why are those separated and why do those use different algorithms, key sizes and lifetimes?
- Use BIND9 tools (dnssec–keygen & dnssec–signzone) or NSD tools (ldns–keygen & ldns–signzone) to secure your zone. Show the configuration files involved and validate your setup (https://dnssec-analyzer.verisignlabs.com, https://dnsviz.net).

Full chain of trust

- Does your parent zone offer secure delegation?
- Describe the DS and DNSKEY records from *sne21.ru* that are important for your domain. Which keys are used to sign them?

Task 4 - Key Rollovers

Zone-Signing Key rollover

- Study RFC 6781 or affiliated online resources
- What are the options for doing a ZSK rollover? Choose one procedure and motivate your choice
- How would you integrate this procedure with the tools for signing your zone? Which timers are important?
- **Bonus (1 point)**: integrate the procedure and use a DNSSec debugger to verify each step

Key-Signing Key rollover

- Can you use the same procedure for a KSK rollover?
- What does this depend on?

Task 5 - DNS-over-HTTPS

Implementing DNS-over-HTTPS on your server.

- For this step you probably will need to recompile and reinstall your server (unbound requires --with-libnghttp2 flag and BIND requires Development Release).
- Also, you will need a certificate for your domain, you can use *certbot* to obtain it.
- Show configuration options that have to be tuned.
- Verify that DNS-over-HTTPS is working (Chrome and Firefox has support for it) by inspecting server incoming queries in the log.

Bonus - Secure Zone Delegation (2 points)

- Securely delegate a subzone to another student - `st<X>.st<Y>.sne21.ru`, where `X` - the number of your machine, `Y` - the number of your partner's machine.
- How to communicate the necessary record to your buddy? (Integrity matters here)
- What about Confidentiality, does it matter here?

Bonus - NSEC vs NSEC3 (1 point)

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.

- What are the main differences between NSEC and NSEC3?
- How to select one or the other during zone-signing?
- Do the root-servers use NSEC or NSEC3? What about the *.org* domain?
- How to take advantage of zone traversal as an attacker, how does it work?