Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

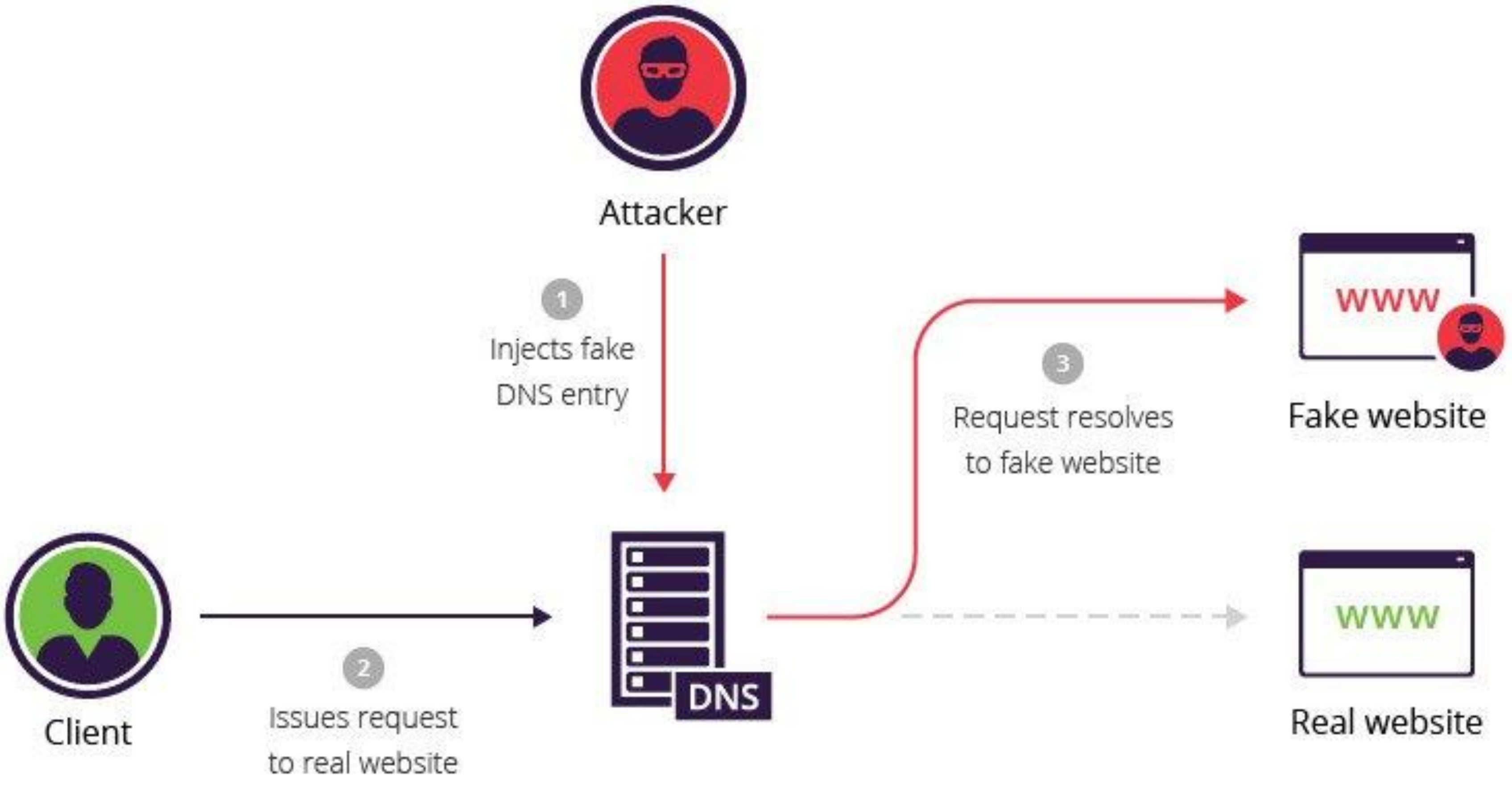
Spring 2025

DNS Security

DNS

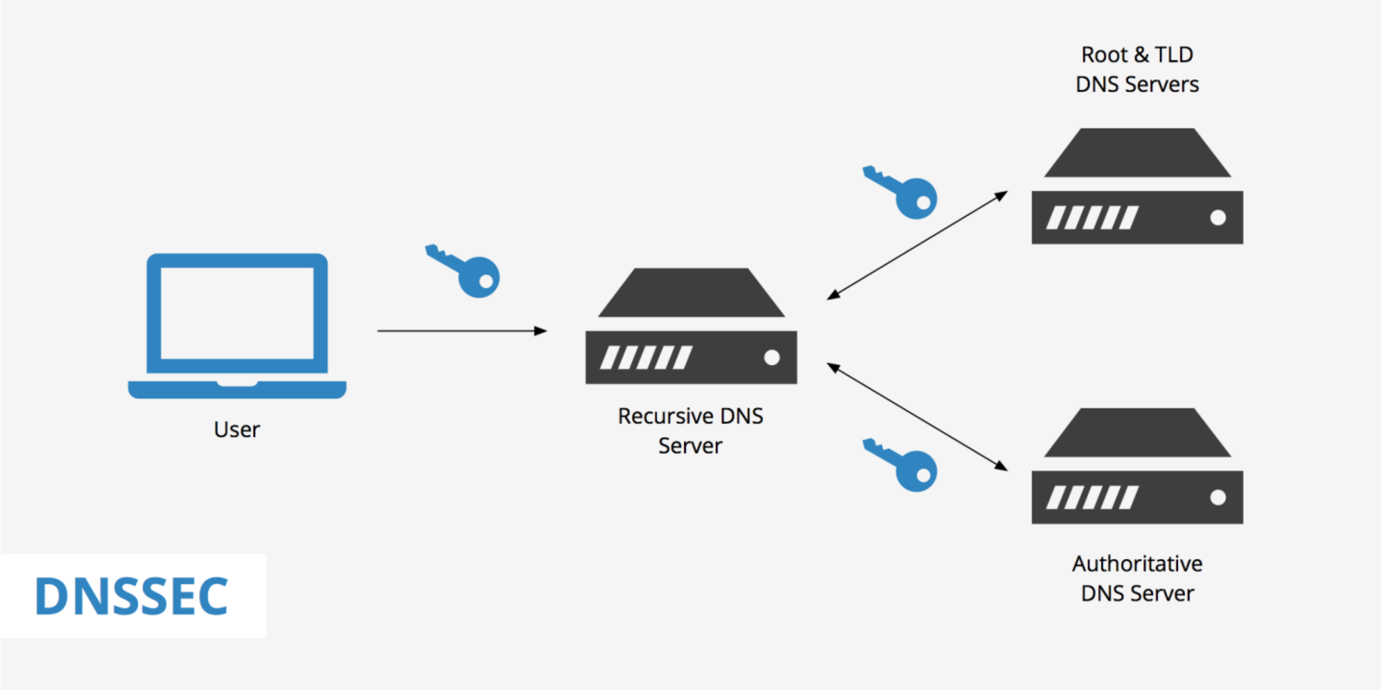
- The Domain Name System (DNS)
- DNS is a hierarchical and decentralized naming system used to translate human-readable domain names
- like www.example.com into IP addresses (like 192.0.2.1)
- DNS use UDP!
- DNS has no encryption!
- Attacks:
  - DNS spoofing ➔ (MiTM)
  - Cache poisoning

DNS Spoofing example



DNS Sec

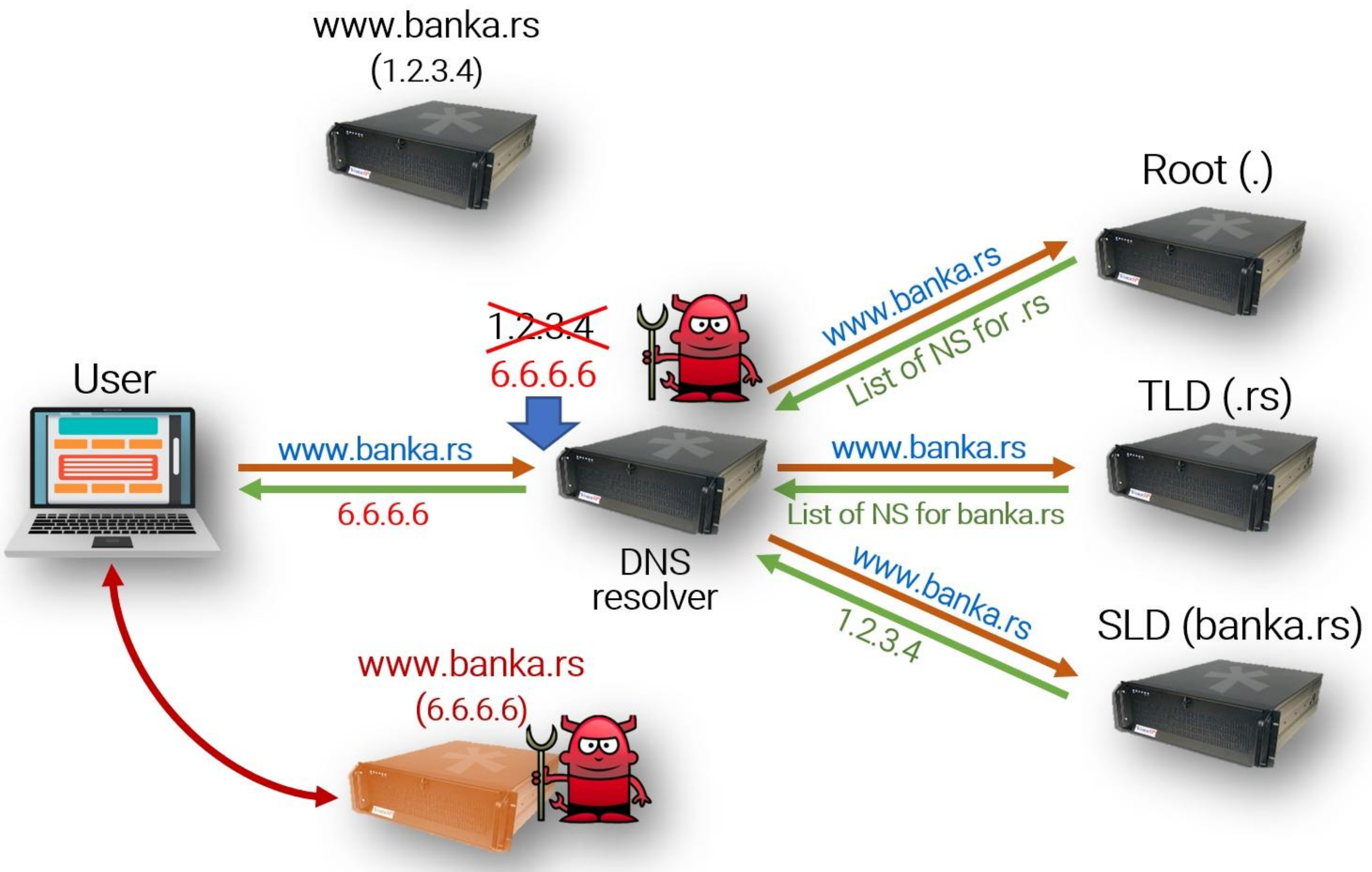
- DNSSEC, or Domain Name System Security Extensions
- is a suite of extensions to DNS that adds a layer of security to prevent certain types of attacks, such as cache poisoning and man-in-the-middle attacks.



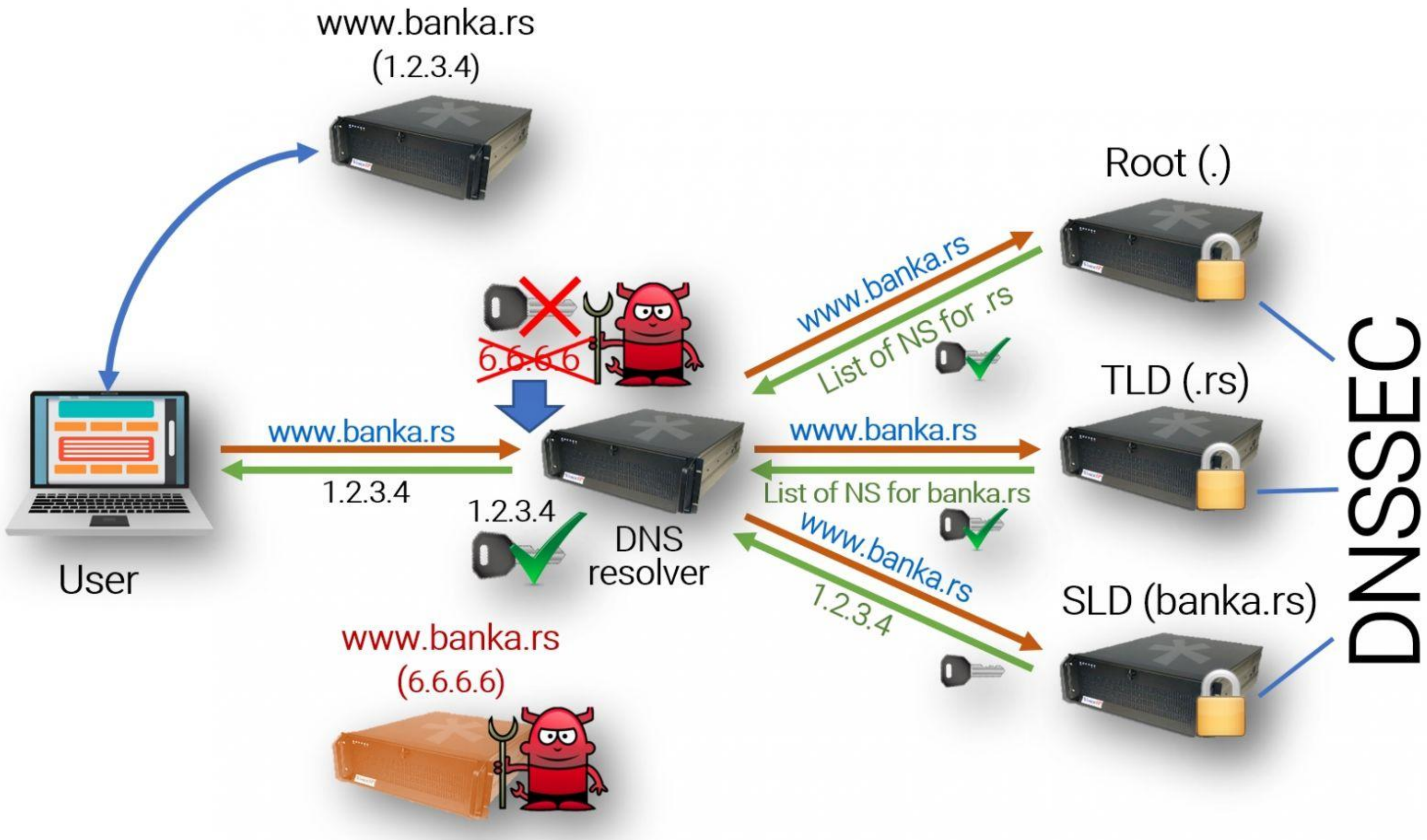
DNSKEY

- A DNSKEY record holds a public key used in the DNS authentication process. When a security-aware DNS resolver receives a DNSSEC response, it retrieves the public key, and uses it to verify the signatures of the rest of the records. An authoritative name server provides a public key, whose matching private key was used to sign those records.

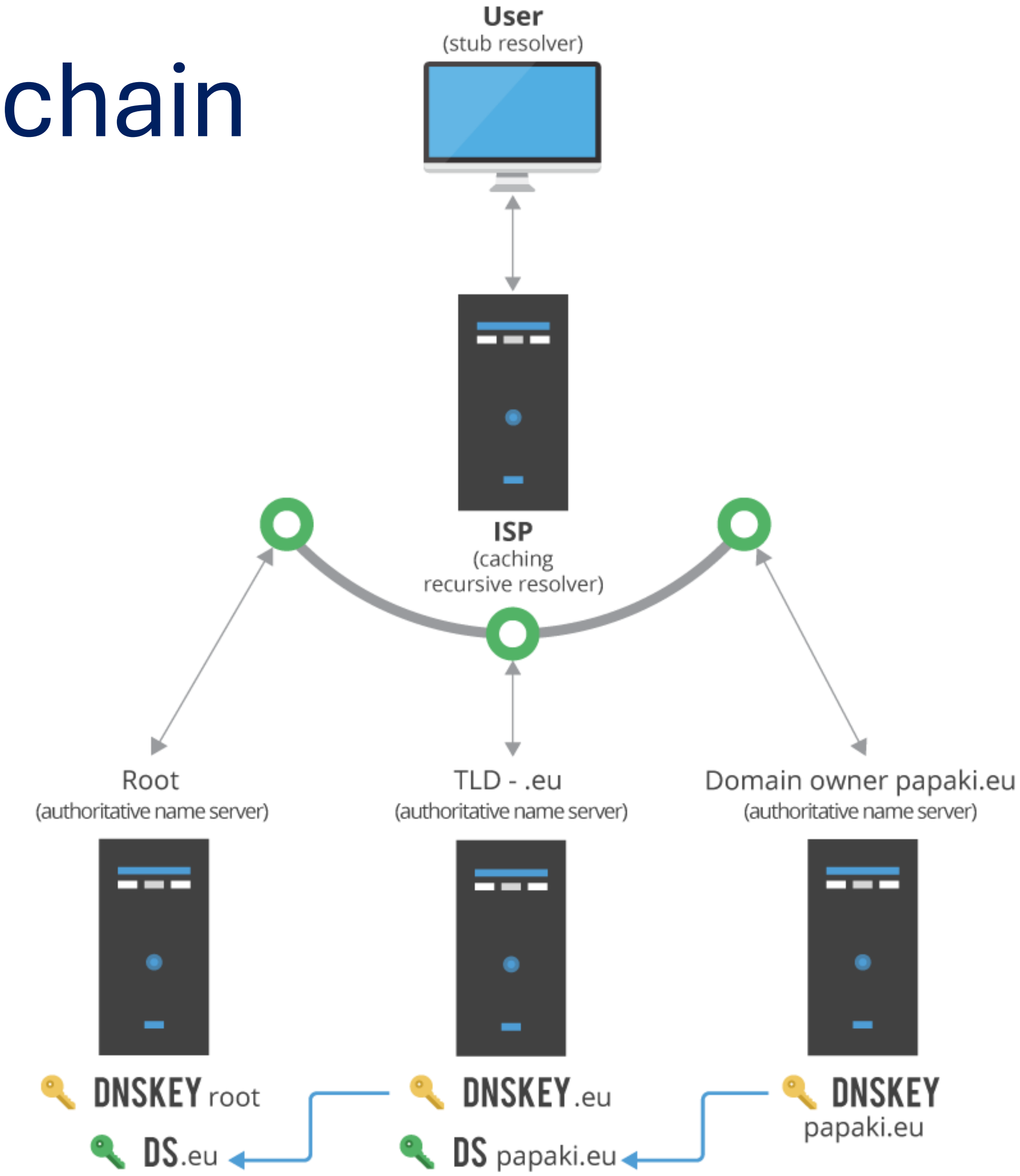
DNS


www.banka.rs
(1.2.3.4)
Root (.)
www.banka.rs
List of NS for .rs
~~1.2.3.4~~
6.6.6.6
User
www.banka.rs
6.6.6.6
TLD (.rs)
www.banka.rs
List of NS for banka.rs
DNS
resolver
www.banka.rs
1.2.3.4
SLD (banka.rs)
www.banka.rs
(6.6.6.6)

DNS Sec


www.banka.rs
(1.2.3.4)
Root (.)
www.banka.rs
List of NS for .rs
6.6.6.6
www.banka.rs
1.2.3.4
1.2.3.4
DNS
resolver
www.banka.rs
List of NS for banka.rs
TLD (.rs)
www.banka.rs
1.2.3.4
User
SLD (banka.rs)
DNSSEC
www.banka.rs
(6.6.6.6)

DNS Sec trust chain



Conclusion

- DNS attacks are very dangerous.
- We must use DNS Sec
- DNS Sec
  - ✓Secure
  - ❖Complex
  - ❖Slow