دانشگاه علم و صنعت ایران

# DNS Security Extensions (DNSSEC): Adoption and Effectiveness

Computer Security

Spring 2025

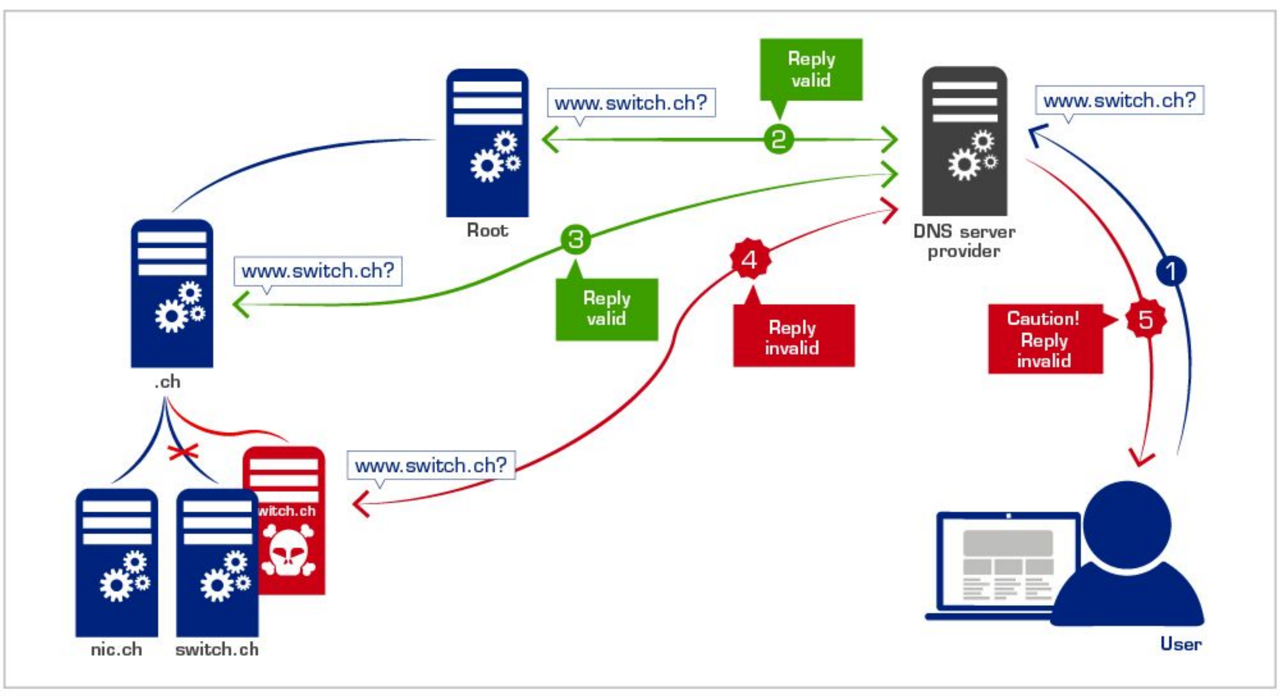
Morteza Malekinejad Shooshtari - 400522211

# Introduction

What problem does DNSSEC seeks to solve?

- How DNS works?
- How attackers could abuse it?
- Which aspects of the CIA triad can we achieve with DNSSEC?
- Is it a brand new protocol?

# An Attack Scenario

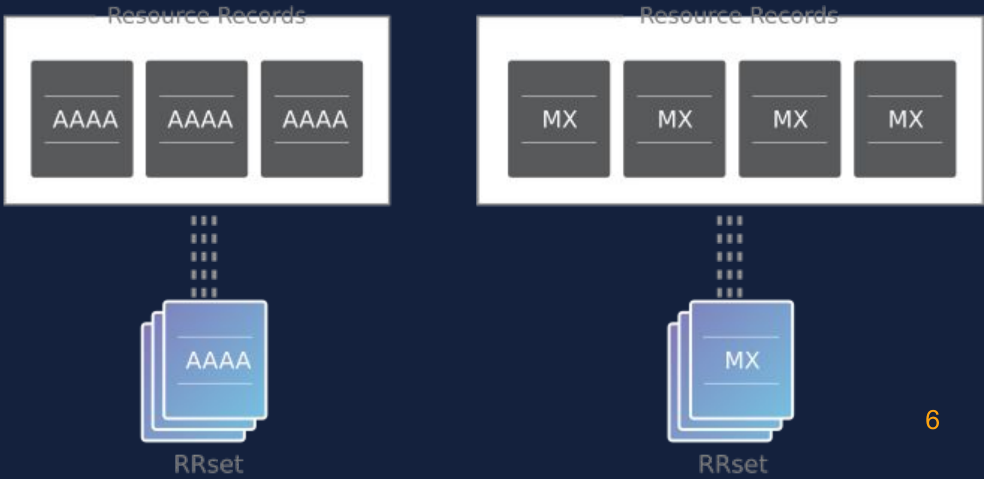


# Methodology

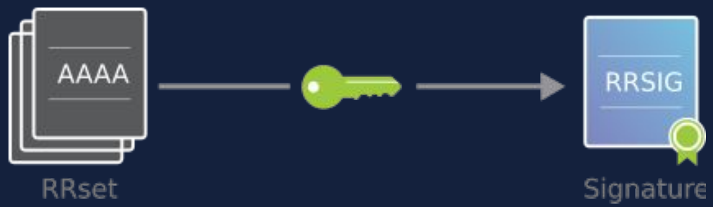
How DNSSEC works

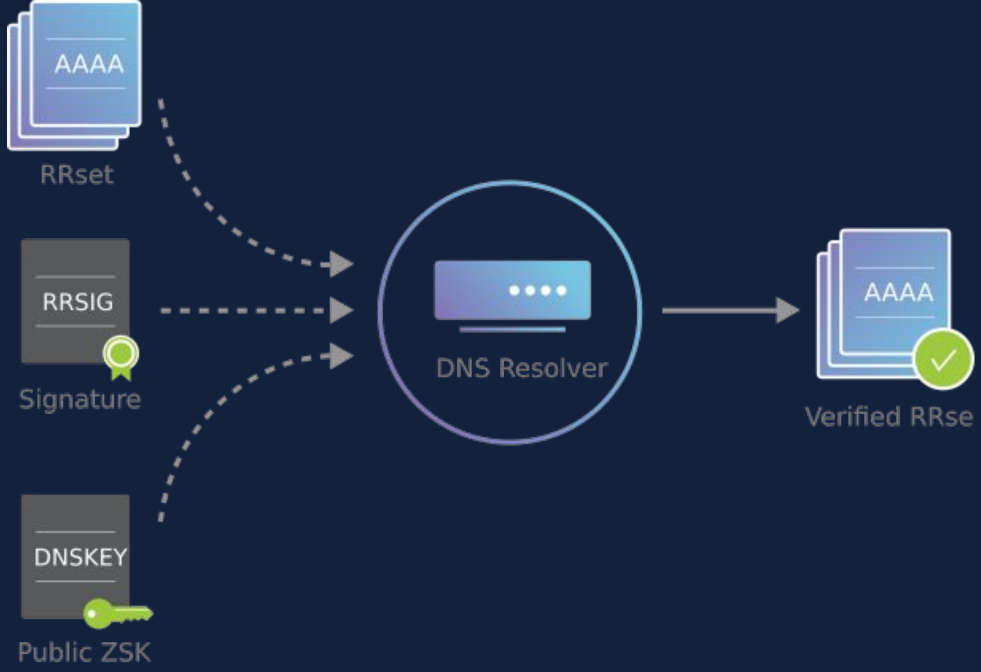
# New DNS record types

- RRSIG - Contains a cryptographic signature
- DNSKEY - Contains a public signing key
- DS - Contains the hash of a DNSKEY record
- NSEC and NSEC3 - For explicit denial-of-existence of a DNS record
- CDNSKEY and CDS - For a child zone requesting updates to DS record(s) in the parent zone.

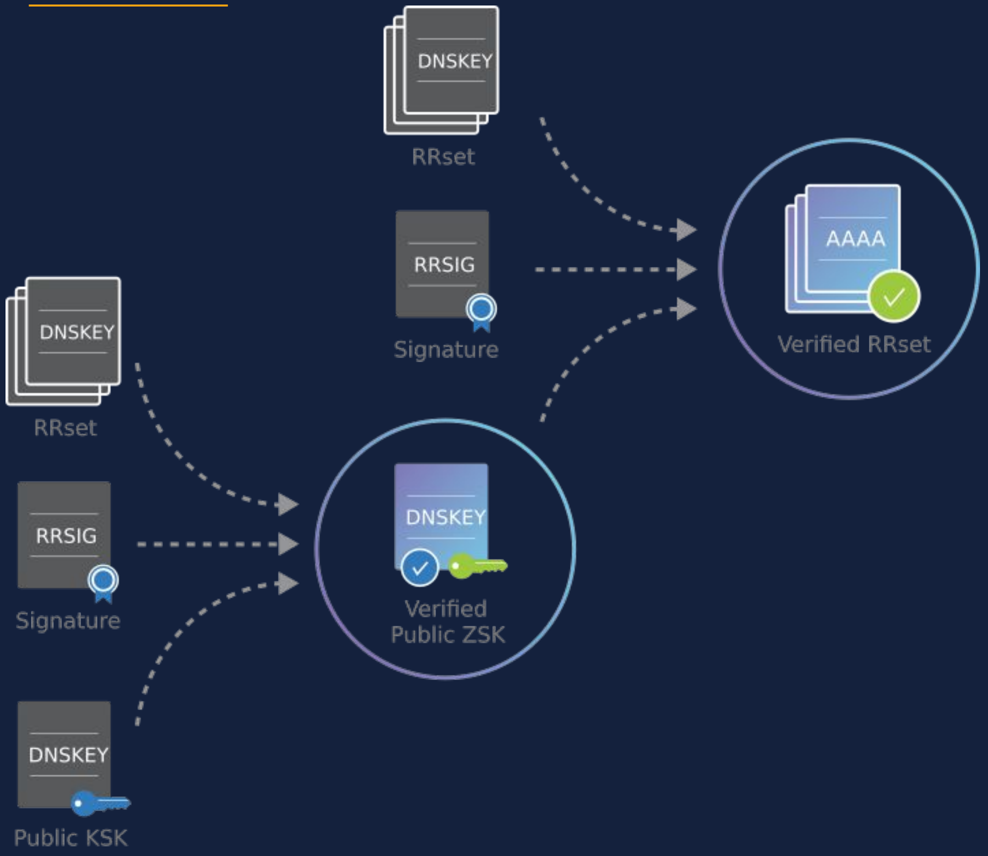


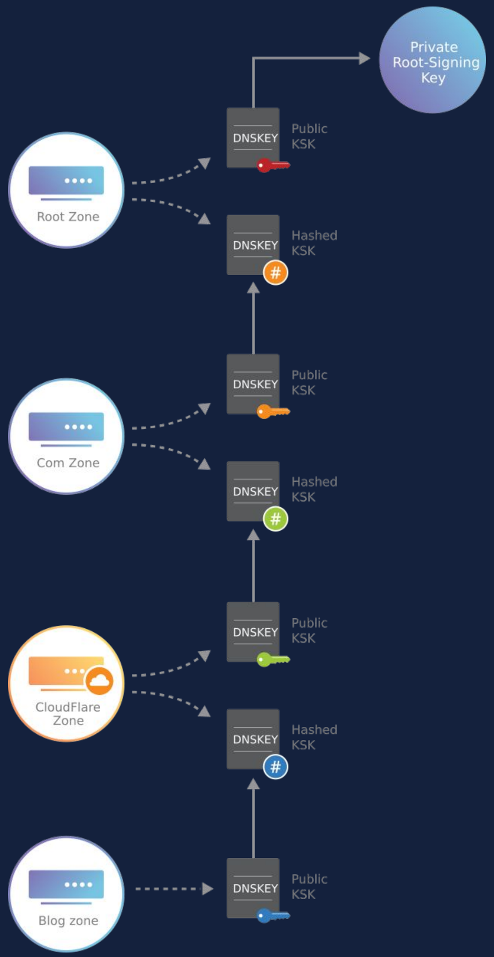
# Signing the records - ZSK





# Signing the records - KSK





# Challenges

- Higher load and CPU usage
  - LBs
  - Prefetch
- Deployment Challenge
  - Complexity (0.45% error on signing!)
  - Monitoring
- Adaptation
- DDoS risks

# References

- How does DNSSEC works? - Cloudflare
- Measurement survey of DNSSEC adaptation
- PREFETCHing to Overcome DNSSEC Performance Issue on Large Resolving Platform
- Deploying and Monitoring DNS Security (DNSSEC)
- A Performance view on DNSSEC migration
- Formal Analysis of the Kaminsky DNS Cache-Poisoning Attack Using Probabilistic Model Checking

# Any Questions?

Thanks.