Cyber Threats in Domain Infrastructure

A Case Study and Takeaways

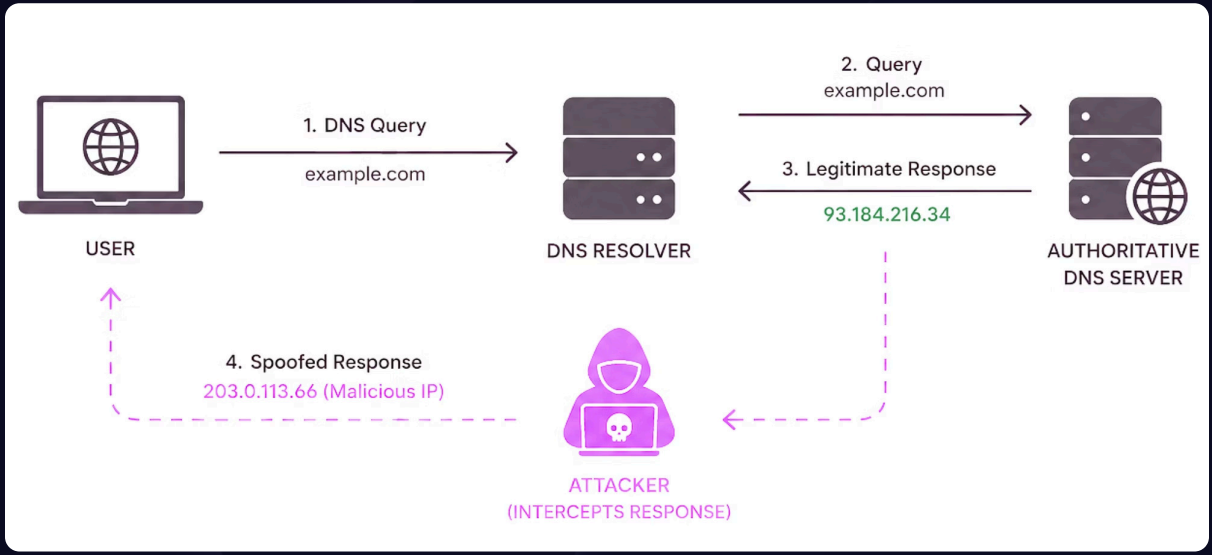
DIANA KOZLOVSKA · ICANN

DNS: The Foundation of the Global Internet

The modern internet depends on DNS to translate domain names into IP addresses, enabling access to websites, email, and cloud services. Yet DNS was designed **without built-in authentication or integrity verification** — creating critical security vulnerabilities.

⚠ Because DNS supports nearly every online interaction, weaknesses at this level pose a **systemic risk** to the stability and trust of the global internet.

DNS Spoofing: A Real-World Attack



How the Attack Works

An attacker injects false DNS records into a resolver's cache, redirecting users to malicious sites — all while appearing legitimate.

- Attacker spoofs responses to ISP resolver
- Resolver cache becomes poisoned
- End users are silently redirected to fake destinations

DNSSEC: The Solution Still Not Widely Used

DNSSEC adds **cryptographic digital signatures** to DNS records, answering one critical question: *"Can this DNS response be trusted?"*

Cryptographic Verification

Digital signatures verify authenticity and integrity of every DNS response.

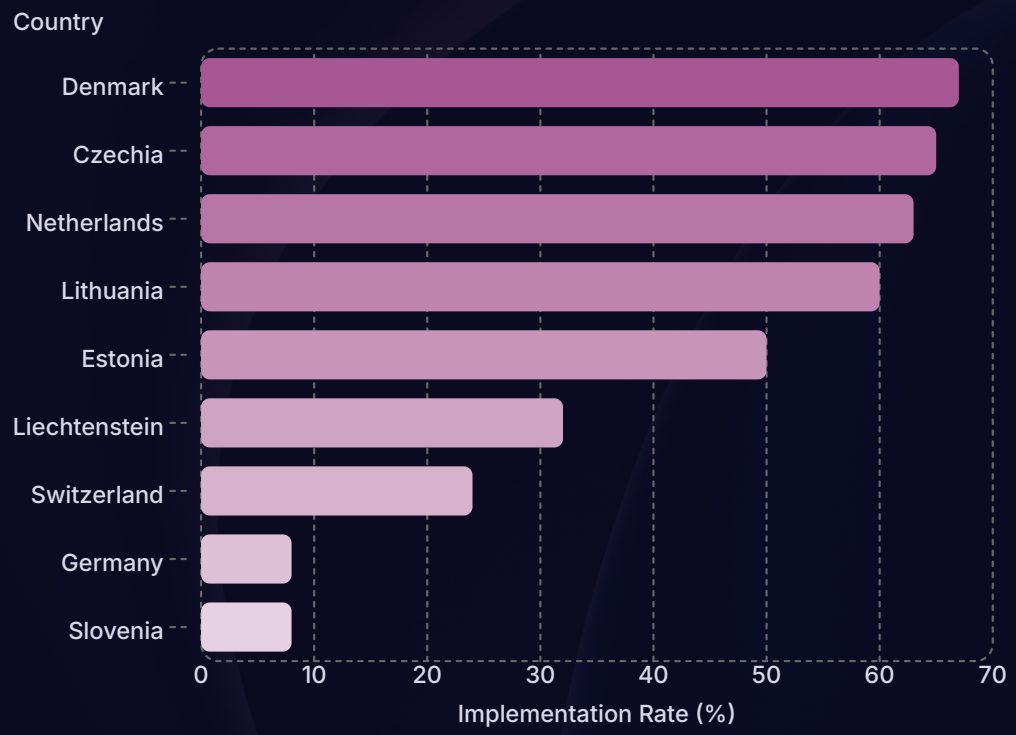
Uneven Adoption

APNIC and ICANN data show DNSSEC deployment remains highly uneven worldwide.

Ongoing Vulnerability

Most internet users still browse without full DNSSEC protection.

Global DNSSEC Implementation Rates (2025)



A Stark Divide

Northern and Western Europe lead adoption thanks to strong cybersecurity policies and modern infrastructure. Sweden and the Netherlands were early adopters.

Many regions still show **critically low validation rates** due to outdated infrastructure and limited cybersecurity investment. APNIC data confirms global DNSSEC validation remains relatively low overall.

Ukraine: A Case Study in DNSSEC Deployment

Ukraine mandated DNSSEC for all **GOV.UA domains** as cyberattacks on state infrastructure intensified — making DNS security a matter of national resilience.

State Resilience

DNSSEC became critical during increasing cyberattacks on Ukrainian state infrastructure.

Secure Communication

Protected official government channels from spoofing and redirection attacks.

Public Trust

Demonstrated that DNS security is directly linked to trust in digital government services.

Why Some Countries Deploy DNSSEC Faster

Fast Adopters

- Investment in digital infrastructure
- Strong cybersecurity regulation
- Government–ISP–registrar cooperation
- Cybersecurity as national strategy

Netherlands and Sweden treated DNS security as strategic priority.

Slower Deployers

- Outdated DNS infrastructure
- Limited cybersecurity funding
- Lack of technical expertise
- Weak public-private coordination

DNSSEC deployment levels reflect a country's overall cybersecurity maturity.

Risks of Ignoring DNSSEC

Slow deployment leaves the internet vulnerable to large-scale DNS manipulation — risks that **increase during geopolitical instability and hybrid warfare.**

Fake Government Portals

Attackers impersonate official sites to spread disinformation or steal credentials.

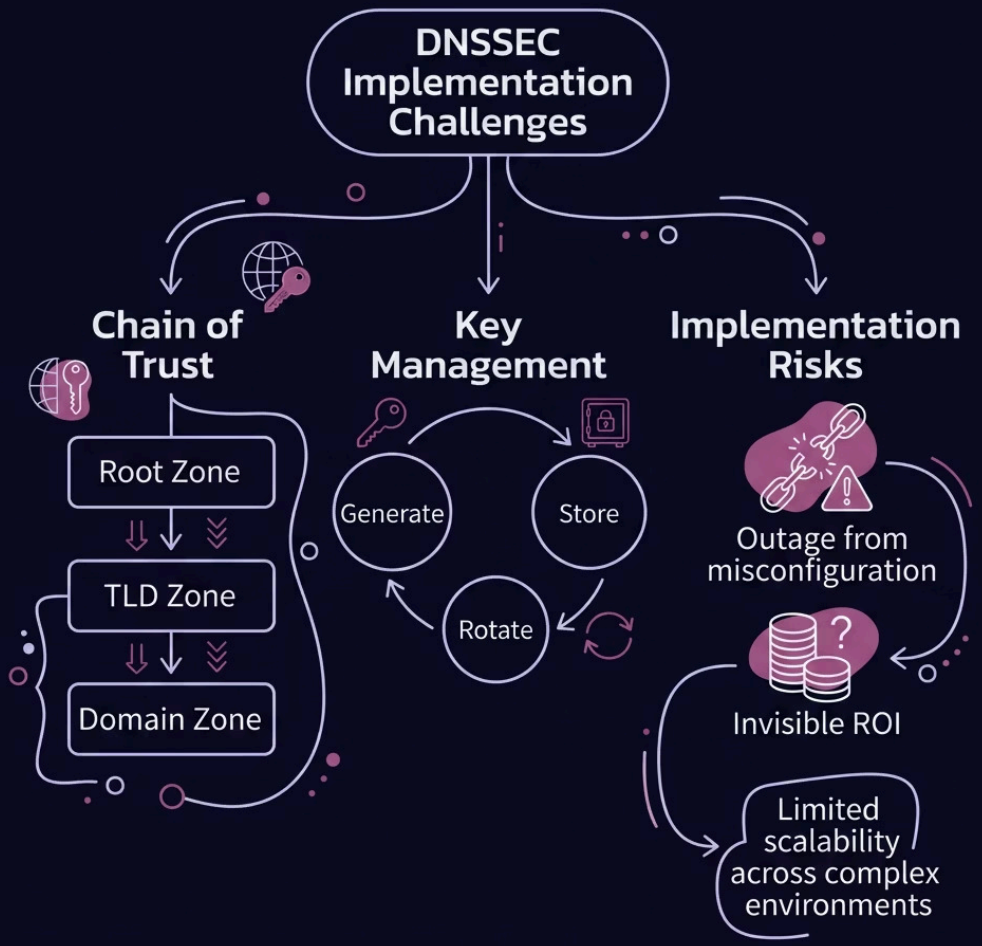
Phishing & Disinformation

Malicious DNS redirection enables large-scale phishing campaigns.

Critical Infrastructure Attacks

Weak DNS enables attacks on financial, energy, and cloud services.

Complexities of DNSSEC Implementation



Key Operational Challenges

- **Service Outages:** Small configuration errors can make websites and networks inaccessible
- **Resource Investment:** Requires continuous monitoring and specialized expertise, raising long-term costs
- **Invisible ROI:** Benefits are preventive, not visible in day-to-day user experience
- **Limited Scalability:** Managing consistent deployment across multiple domains and teams is difficult

Areas of Improvement & Key Takeaways

The central goal: **shift DNSSEC from optional technology to mandatory cybersecurity requirement.**

01

Mandate for Critical Resources

Require DNSSEC for all government and critical state digital infrastructure.

02

Expand ISP Validation

Internet service providers must enable DNSSEC validation across their networks.

03

Strengthen Regulation

National cybersecurity policies must support and enforce wider DNSSEC adoption.

04

Raise Awareness

Organizations and users need greater education about DNSSEC and its importance.

Key takeaway: DNS does not guarantee trust — DNSSEC addresses this vulnerability, yet it remains under-implemented globally. Progress requires policy, infrastructure investment, and regulation working together.

Thank You for Listening

Diana Kozlovska · ICANN

Cache Poisoning Vulnerabilities in DNS

Bailiwick Checking Weaknesses

Bailiwick checks are meant to block replies from non-authoritative sources. Implementation flaws can let attackers slip poisoned responses into caches.

Unvalidated Cache Reuse

DNSSEC troubleshooting can bypass validation and store forged data. That bad data may then be reused in normal lookups.

Crypto Agility Attacks

Resolvers may skip validation when they encounter unsupported algorithms. Attackers can exploit this downgrade path to feed unsigned answers.

Persistent DoS via Cache Injection

A single poisoned record can linger for a long time. The result can be widespread DNS failure and prolonged outages.

Advanced: DNSSEC Cache Protection Mechanisms

Aggressive NSEC/NSEC3 Caching

- Generate negative answers from cached NSEC records
- Prevents unnecessary queries to authoritative servers

Wildcard Synthesis

- Synthesize answers from cached wildcard records
- Reduces query load on authoritative servers

Performance Gains

- Reduces latency and round-trip time
- Decreases resource utilization across DNS infrastructure

Privacy Enhancement

- Fewer queries to authoritative servers
- Protects user query patterns from exposure

Cache Protection Effectiveness: Key Metrics

40%

Reduction in Resolver Queries

Aggressive NSEC/NSEC3 caching eliminates unnecessary queries to authoritative servers

60%

Latency Improvement

Wildcard synthesis and cached responses reduce round-trip time for DNS lookups

75%

Resource Utilization Decrease

Combined effect of caching mechanisms reduces load on both recursive and authoritative servers