

DNSSEC protections are doing better than you'd think!

Quan Nguyen

George Mason University

qnguye31@gmu.edu

Eric Osterweil

Verisign

eosterweil@verisign.com

DNSSEC from another perspective

- DNS was designed like a “phonebook” **mapping** names to IP address.
 - Evaluations have focused on the service mappings.
- DNSSEC added protections by protecting **objects** that map to services
 - But, evaluations of service mappings don't speak to how well objects are protected by DNSSEC.
- So, how **well** have DNSSEC *objects* been **protected**?
 - Our novel framework measures and evaluates the protections of DNSSEC objects.
- Using our framework, we found that DNSSEC objects have been well protected over the last 10 years.
 - 99% of DNSSEC objects had 99.999% integrity protections, and
 - 91.6% had 99.999% consistent origin authentication.

Outline

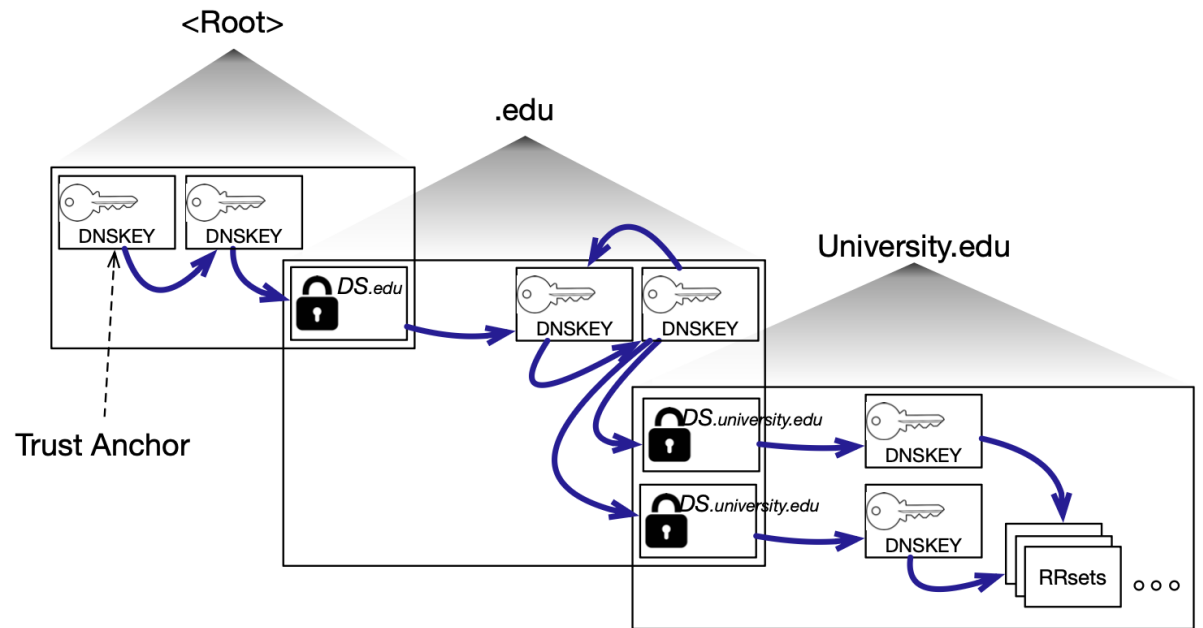
- Service sets vs. protections
- Protection models and Measure of Protection (MOP)
- DNSSEC's Authentication protections
- Discussion

Two aspects of security protocols

- Fundamental observation: when implementing security *over time*, service sets are different from protection.
 - Transmission security vs. object security.
- Service sets:
 - Origin authentication [RFC4033]
 - Integrity assurance services [RFC4033]
- Protections:
 - Effectiveness of protections over time.
 - E.g.: was an object's name can be authenticated the whole time?
 - Also needs to be monitored and evaluated.

Protection Models

- “Threat models” specifies **threats** and evaluates compromises.
- Protection models captures “what needs to be **protected**.”
 - E.g.: RFC specifies objects need to have authenticable names by the chain of trust.
 - But, is there always a verifiable path over an object’s lifetime?



Protection Models (2)

- Lends itself into a **measurement**, which we refer to as a Measure of Protection (MOP).
- Verifiability protection model
 - Objects' domain names should be authenticatable consistently.
 - Fraction of an object's lifespan during which it is authenticable.
 - Five-nines?
 - Always have *at least one* verifiable path in the chain of trust.
 - Implicitly, always have at least one verifiable path within the zone.
- Different protection models will require different measurements.

Measure of Protection (MOP)

- What needs to be measured to **quantify** how well objects have been protected.
- May need to measure more than one thing/aspect.
 - A MOP is usually multi-dimensional, i.e. a tuple.
- Can be defined mathematically in closed forms.

Measure of Protection (MOP) (2)

For DNSSEC's authentication protection:

$$MOP_{auth} = (\bar{v}, \bar{d}_{down}, \bar{d}_{up}, \check{l}_z, \tilde{l}_z, \check{l}_p, \tilde{l}_p)$$

- $\bar{v}$ is the *mean* verifiability of an *object's name* over an object's lifetime.
 - $\check{l}_p$ is the **minimum** number of verifiable paths in the chain of trust ever existed over an objects' lifetime.
 - $\check{l}_z$ is the **minimum** number of verifiable paths in the chain of trust ever existed over an objects' lifetime.
-
- A straw man for Verifiability protection model
 - $\bar{v} \geq 0.99999$
 - $\check{l}_p \geq 1$ and $\check{l}_z \geq 1$

Evaluation

- Data from SecSpider database.
- 9.4 M DNSKEY objects.
- 91.6% of objects are protected under the verifiability protection model.

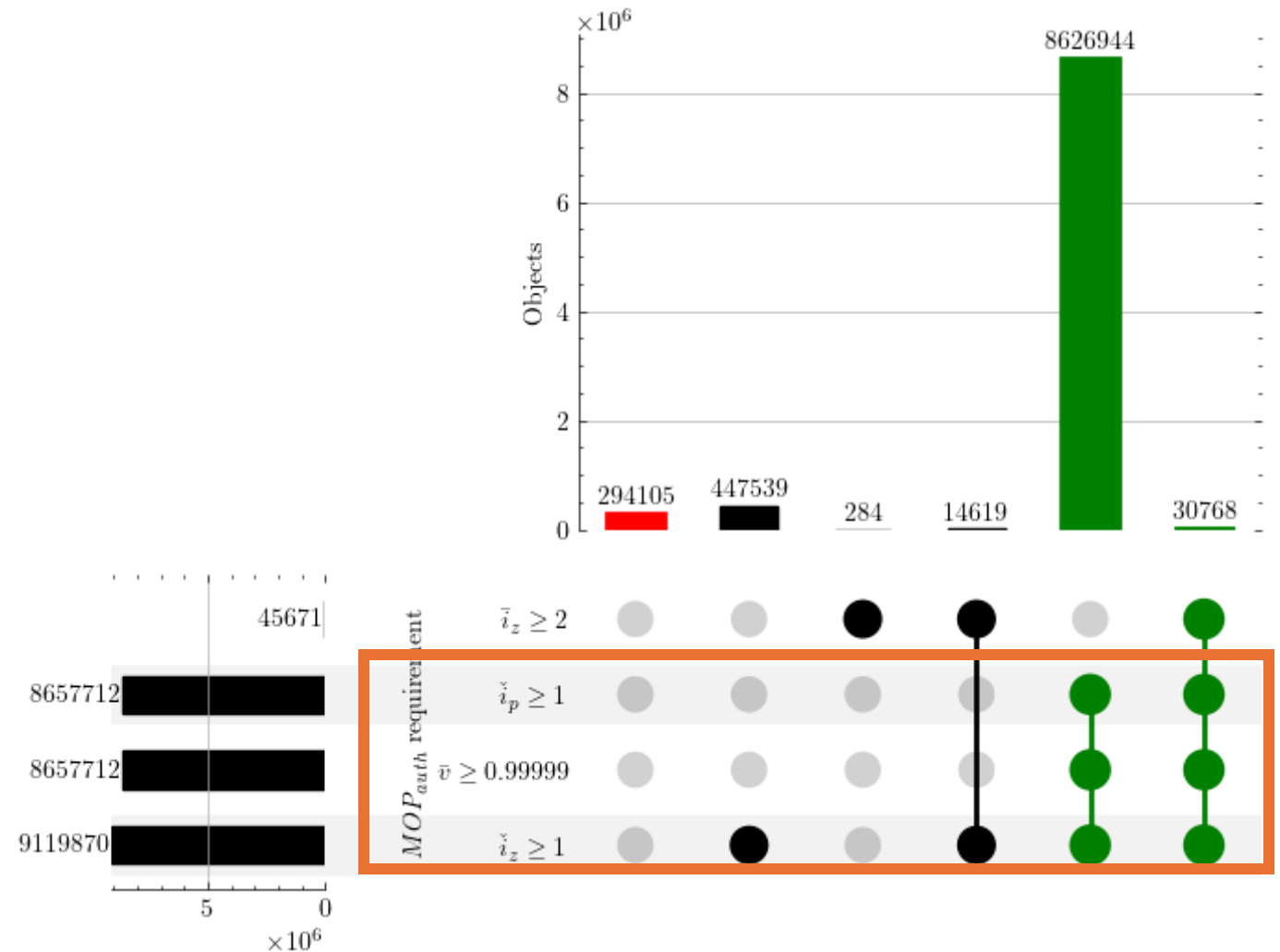


Figure 1: The UpSet plot showing the counts of objects categorized by MOP_{auth} straw man requirements

Discussion

- Positive results: across all DNSSEC-enabled zones in the world, 91.6% of objects had five-nines consistent authentication.
 - Additionally, 99% met five-nines integrity protections (not discussed due to brevity).
- Indication that DNSSEC is well run loosely federated security system.
- Other benefits of our methodology:
 - Allows interested parties to quantify and evaluate protections of objects.
 - Applicable to other object security protocols (by specifying different protection models and thus, different MOPs).
- Work under submission. Please reach out for more details.

Thank you for listening!