Evaluating Multi-Signers using Independent Point of Failure (IPF) Protection Model

Quan Nguyen, Eric Osterweil

George Mason University

{qnguye31, eoster}@gmu.edu

Motivation

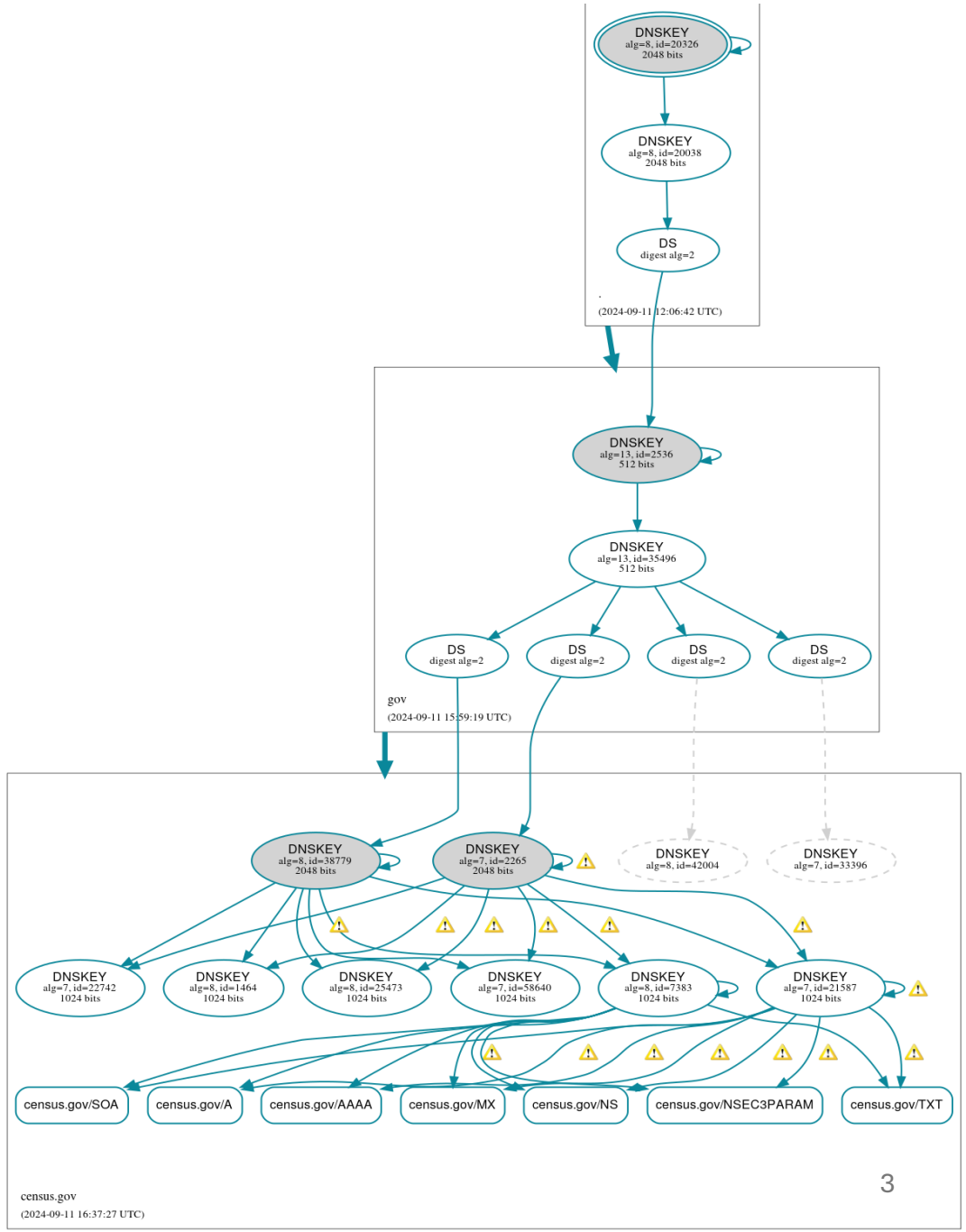
- Zone operators using DNSSEC to protect their zones with signatures, there must be some **signers**.
- What if the single **signer failed** catastrophically?
  - E.g.: not being able to operate, providing bogus signatures, or being compromised, etc.
  - Zones become unprotected and might even take an **outage**.

- From our measurements, a lot of zones have deployed a lot of crypto to increase redundancy.
- But how protected are they?

Chain of Trust as a Directed Graph

- Example zone: census.gov.
- Crypto verification paths form a **directed graph.**

- A lot of redundancy!



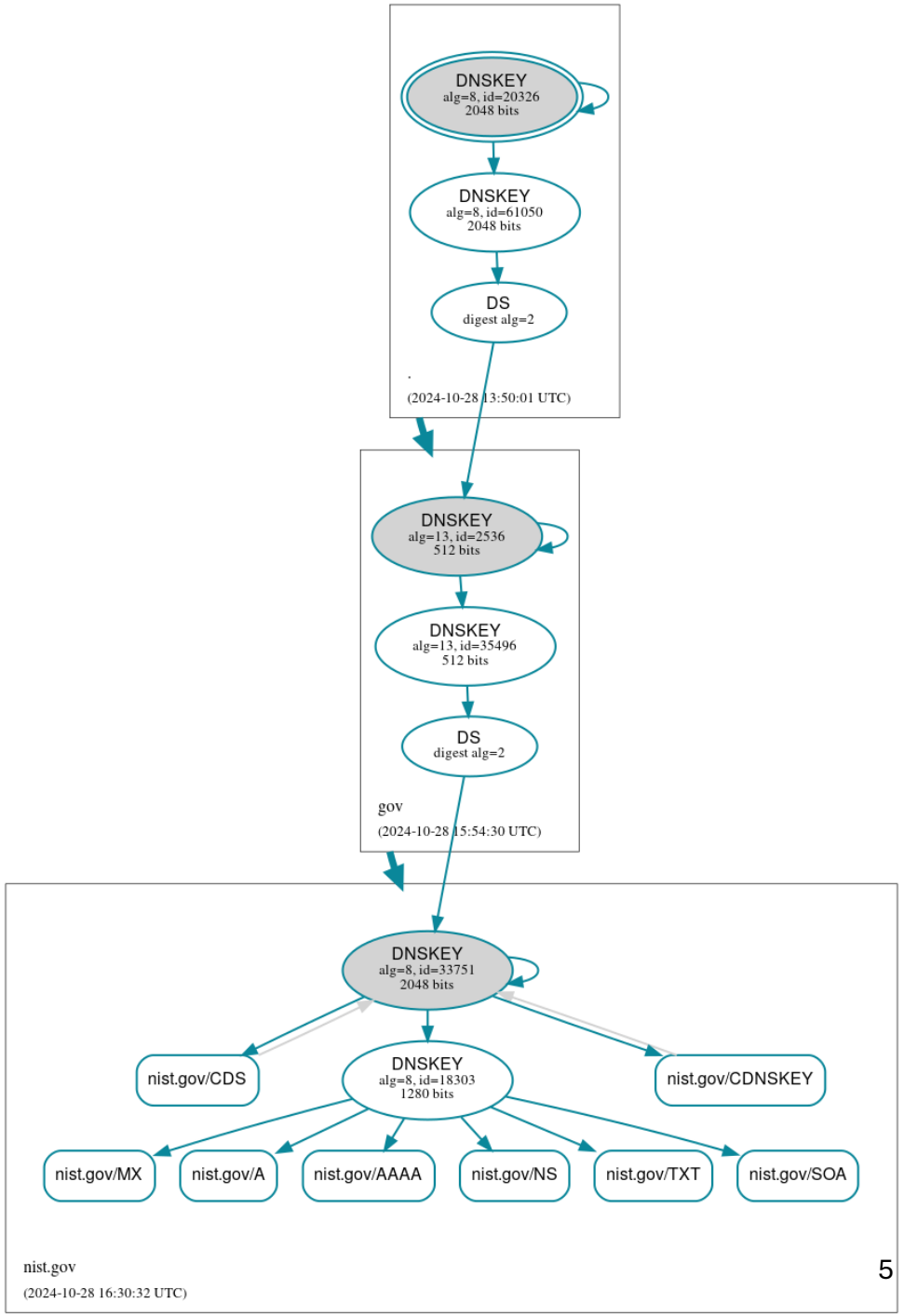
What really matters?

- Does that much crypto redundancy actually help a zone?
  - Is it translating to extra security?
  - Is redundancy resilient against failures from single signers?

- We need a way to **quantify** how protected zone is for the amount of crypto they invest in.
  - More is not always better!

IPF Protection Model

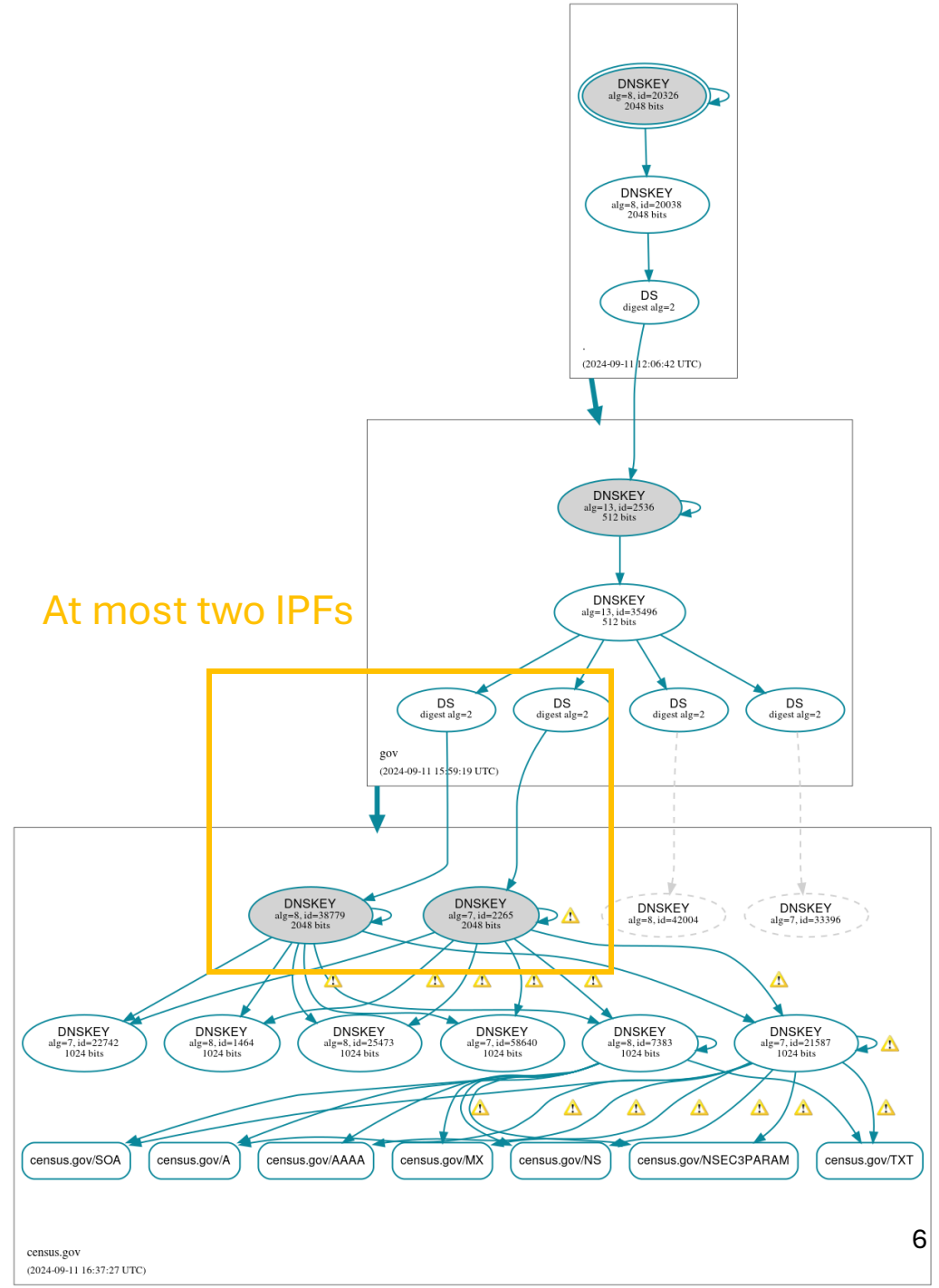
- Measure security as how many **single points of failure** a zone has.
  - We measured independent points of failures (IPFs).
- IPFs as a measure of a zone's resiliency (against single point of failure).
- IPFs ~ vertex-disjoint paths in the directed graph.



Reflecting back to census.gov.

- Starting from the delegation, the zone has 2 IPFs.
- Going up the chain, they become 1 IPF.

- Census.gov has heavily invested in its redundancy.



Preliminary Measurements

- Measuring **longitudinal DNSSEC** data from the SecSpider database.

- Many zones deploying **extreme amount** of crypto, but resulting in **little functional security.**
- Path IPFs are **limited** because they are highly dependent on the predecessors.
- E.g.: Geo.census.gov had 100+ M feasible verification paths at some point, but only ever had one IPF.

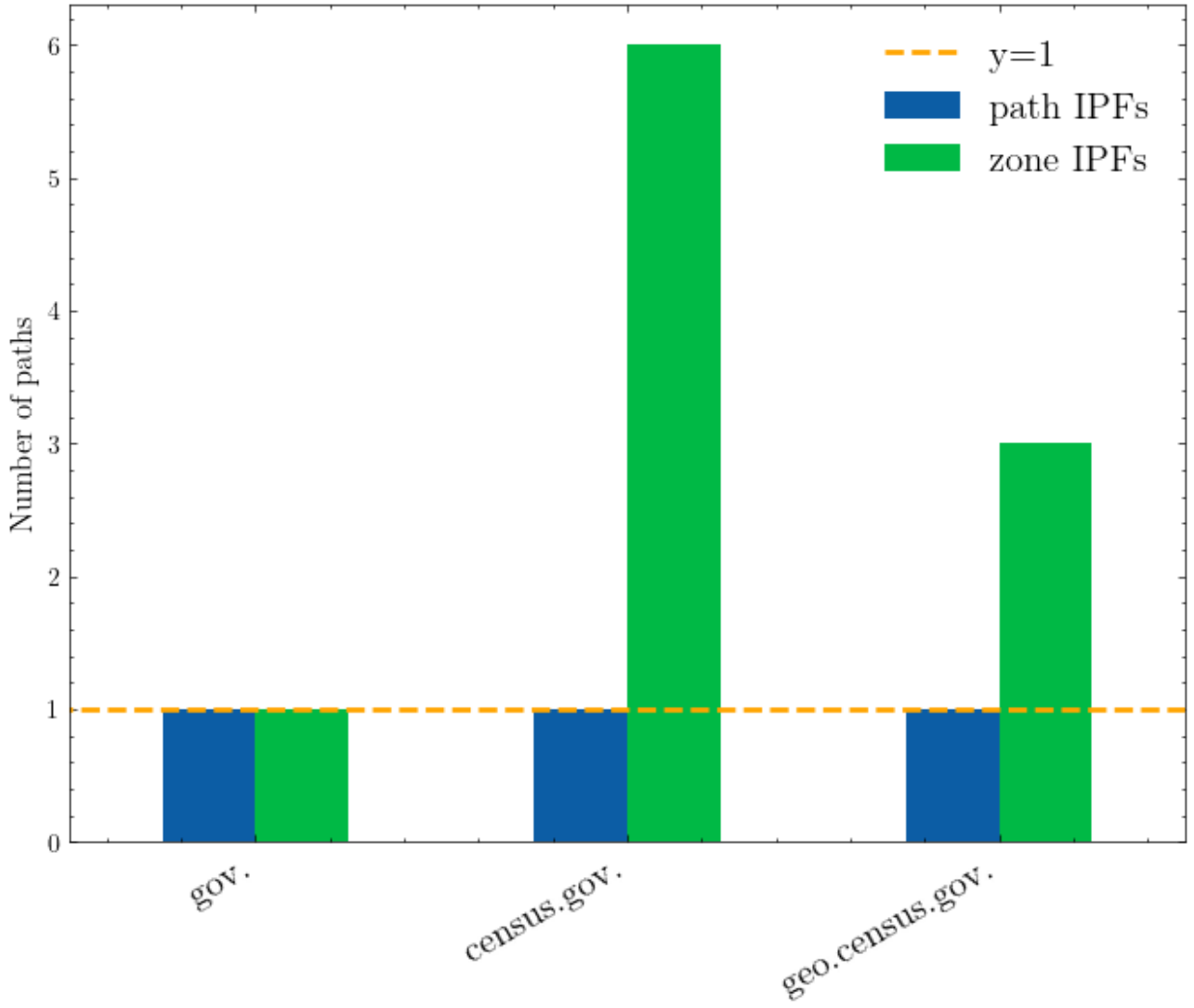


Figure 1: Highest number of IPFs we observed.

Wrapping Up

- IPFs are a concrete example of quantifying protection.
  - IPFs quantify how much of the deployed crypto are working in **a meaningful way.**

- On going work:
  - Combing through 20 years of DNSSEC deployment to see how much protection DNSSEC actually been affording different zones. How often have they been limited by their predecessor graph?
  - Analyzing and proposing data-driven practices of signing zones that result in **functional security**.

We welcome any comments or feedback!

Contact info:

Qnguye31@gmu.edu

Eoster@gmu.edu