

The State and Challenges of the DNSSEC Deployment

Eric Osterweil

Michael Ryan

Dan Massey

Lixia Zhang

Monitoring Shows What's Working and What needs Work

- DNS operations must already deal with widespread misconfigurations and errors
- DNSSEC adds a significant amount of complexity to plain-old DNS
- In this talk we show evidence that the DNSSEC deployment is gaining ground

- and -

evidence that DNSSEC's complexity is becoming visible in crypto management and the delegation hierarchy

Outline

- DNSSEC primer
- Growth of DNSSEC
- Crypto Management
- Crypto is a Challenge Faced by DNSSEC
- Conclusion

DNSSEC Primer

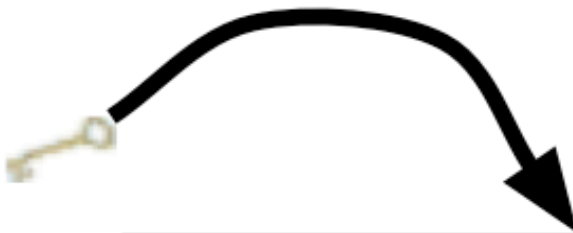
- DNSSEC provides *origin authenticity*, *data integrity*, and *secure denial of existence* by using public-key cryptography
- Origin authenticity:
 - Resolvers can verify that data has originated from authoritative sources.
- Data integrity
 - Can also verify that responses are not modified in-flight
- Secure denial of existence
 - When there is no data for a query, authoritative servers can provide a response that proves no data exists

How DNSSEC Works

- Each DNSSEC zone creates one or more pairs of public/private key(s)
 - Public portion put in DNSSEC record type DNSKEY
- Zones sign all RRsets with private key(s) and resolvers use DNSKEY(s) to verify RRsets
 - Each RRset has a signature attached to it: RRSIG
- So, if a resolver has a zone's DNSKEY(s) it can verify that RRsets are intact by verifying their RRSIGs

Signing Example

Using a zone's key
on a standard RRset (the NS)



```
secspider.cs.ucla.edu. 3600 IN NS zinc.cs.ucla.edu.  
secspider.cs.ucla.edu. 3600 IN NS alpha.netsec.colostate.edu.
```

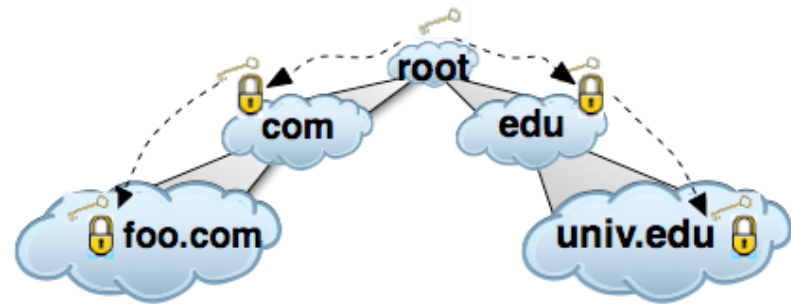


Signature (RRSIG) will
only verify with the
DNSKEY if *no* data
was modified

```
secspider.cs.ucla.edu. 3600 IN NS alpha.netsec.colostate.edu.  
secspider.cs.ucla.edu. 3600 IN NS zinc.cs.ucla.edu.  
secspider.cs.ucla.edu. 3600 IN RRSIG NS 5 4 3600 20080324024800 (  
20080322024800 44736 secspider.cs.ucla.edu.  
E4msde1nzV1fGwDo2X6jLU5d9Xrk371rYRCZN6yq5ad  
mABa3B3KgK113u2VBXDuJZuchSwPQMBy+J0motZ0ggf  
SgQUUYm86v8G7ABHHcI+YFD3z3eqSoAoBAE5ysafop1u  
g7tw1J4xd/IADIVeu1HnVIKRSycILXzvCwcaDwAd610  
9oJUBSMgWZjGzYeJ09Rz0oUUqIqtn9PgV0zdTm+WnRC3  
LEz50fdoP743QvPhe7RrF9w1KA3M0ptTiQA++W8Gg085  
NhbJ7MD99nEYaEv3+GuDCTkCy5Z0WoI/2Bcjq1NGBDLo  
71lo6udu72i1tpyRfTEEQuirpInlZ9+IMw== )
```

Getting the Keys

- Until a resolver gets the DNSKEY(s) for a zone, data can be spoofed
- How can a resolver know that the DNSKEY(s) *themselves* are not being spoofed?



- DNSSEC zones securely delegate from parents to children
- Zones that have no secure parents are called trust anchors
- When a zone is a trust anchor the zones that it delegates to form an *island of security*

Measurements from SecSpider

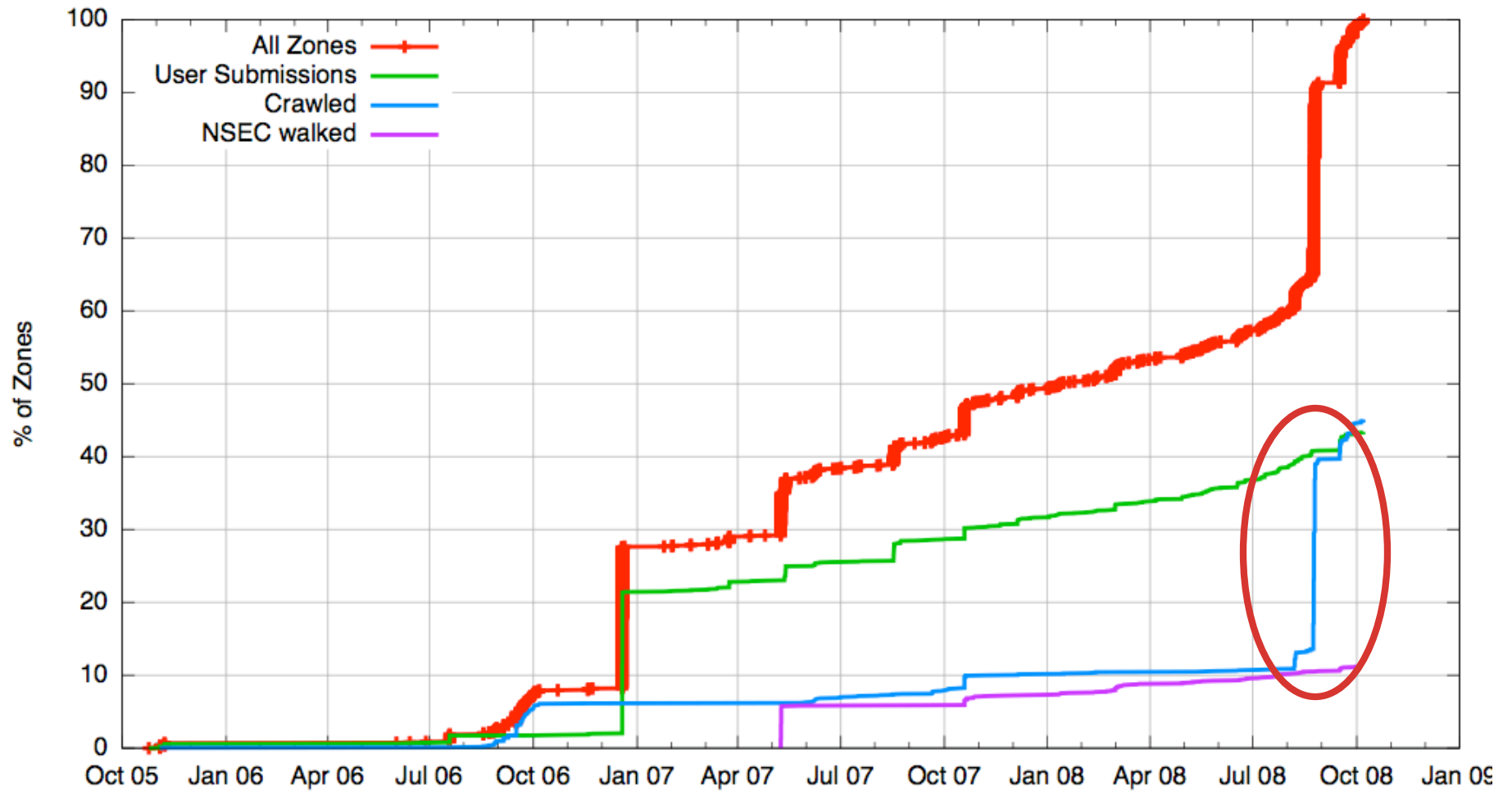
- SecSpider is the first DNSSEC monitoring project
 - Began late in 2005
 - Zones taken from user submissions, various crawling engines, and NSEC walking
- Monitoring over time from distributed locations has allowed us to:
 - Observe the deployment's growth
 - Study distributed inconsistencies
 - Study policies and general behavior of early adopters

Production Set

- Zones are classified as production iff they:
 - Are under arpa
 - Reverse mappings - 160.96.179.131.in-addr.arpa
 - Or, are a TLD
 - com, edu, se, de, bg
 - Or, maintain a reachable web server at a www domain
 - Or have a mail server listed under an MX
 - We currently track 1,627 production DNSSEC zones

Growth of DNSSEC

CDF of DNSSEC zones

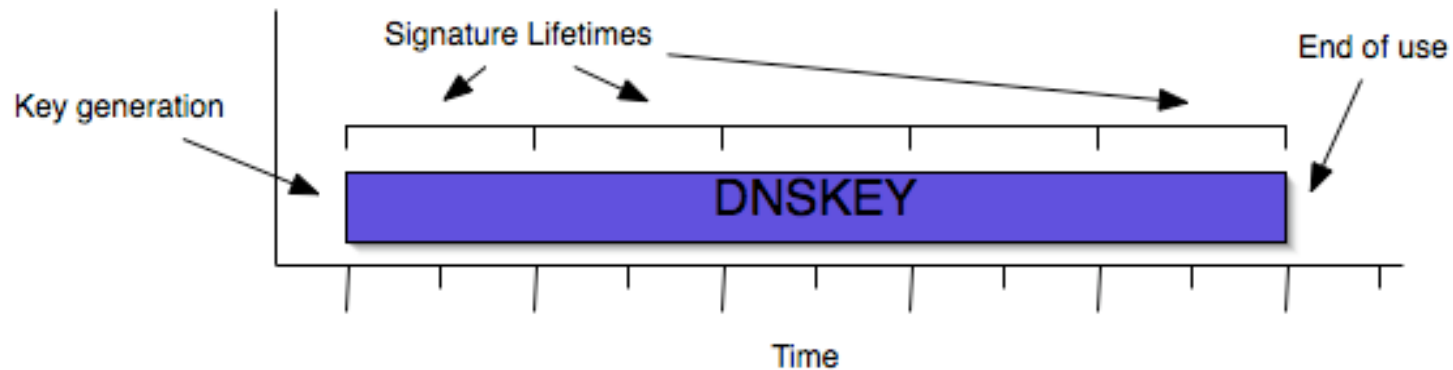


Crypto Management

- Having keys and creating signatures can be more involved than it first seems
- Paul Mockapetris, SIGCOMM'88:
“Distributing authority for a database does not distribute a corresponding amount of expertise.”
- We, therefore, posit that:
“Deploying cryptography for a database does not deploy a corresponding amount of expertise.”

Key vs. Signature Lifetimes

- There is a distinct difference between the signature lifetimes of DNSKEYs and the actual period of use
 - A key with a short signature lifetime can be re-signed indefinitely!

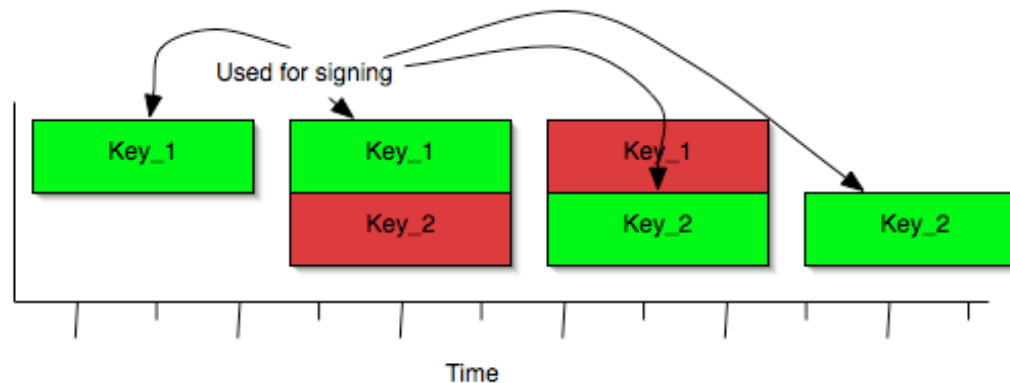


Signature vs Actual Lifetimes

- Signature lifetimes -> Actual average lifetime
 - 0-30 days -> 102.651 days
 - 31-60 days -> 68.9527 days
 - > 60 days -> 395.085
- Pruning keys that have not expired yet
 - 0-30 days -> 83.2043 days
 - 31-60 days -> 209.19 days
 - > 60 days -> 156.762 days
- Key lifetimes are clearly different than signature lifetimes

How Keys *Should* be Changed

- When Key changes are needed, old keys need to overlap with new keys
- We call these *chained rollovers*
- Sign with Key_1 -> add Key_2 -> Sign with Key_2 -> Stop serving Key_1

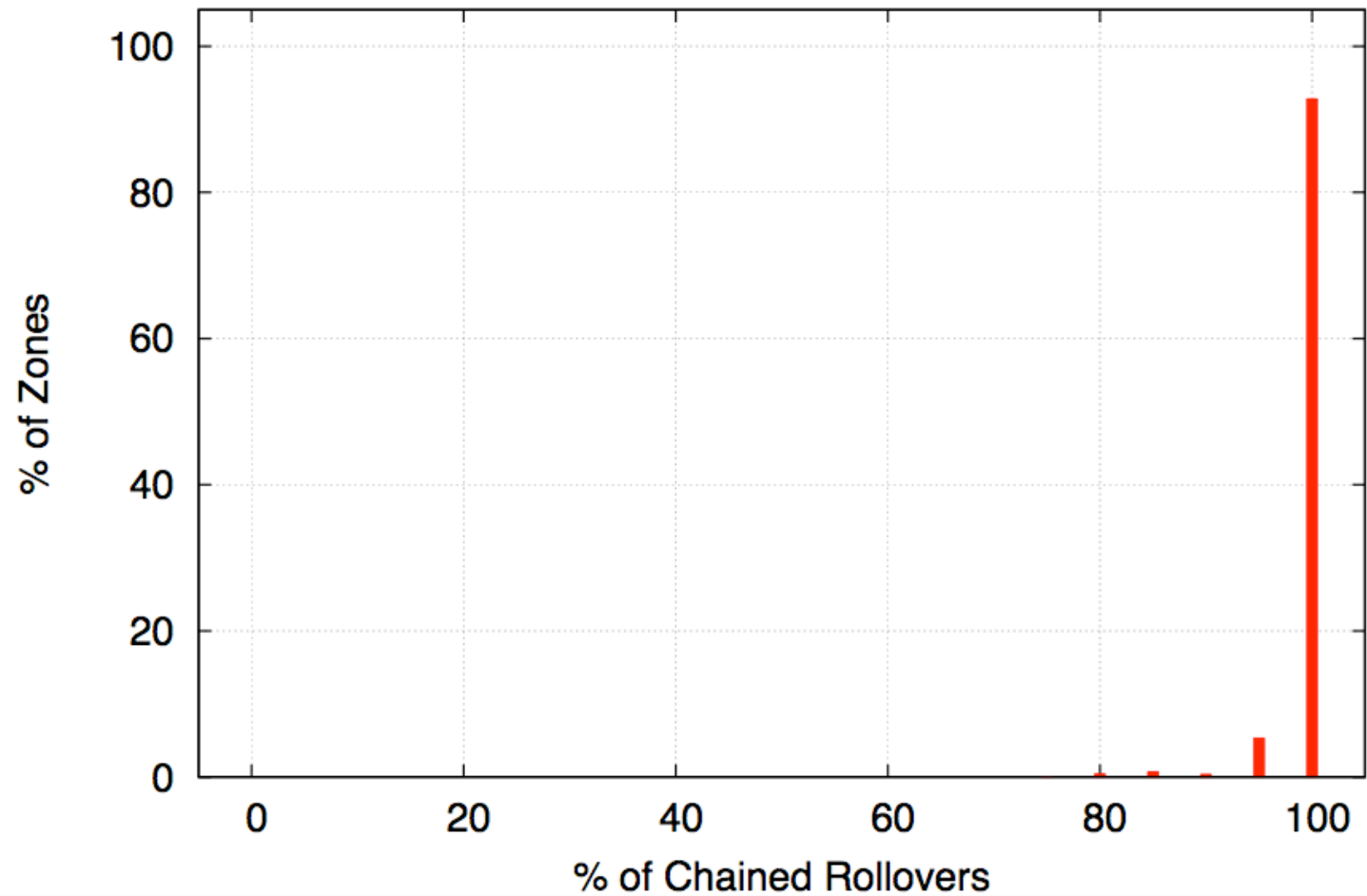


Otherwise...

- Abrupt key changes may leave signatures from old keys in caches
- Resolvers may not be able to verify data with an old signature and a new key
- That is why key changes must be chained
 - Until all signatures from a key have expired, a zone must serve that key, or resolvers may encounter data that seems false

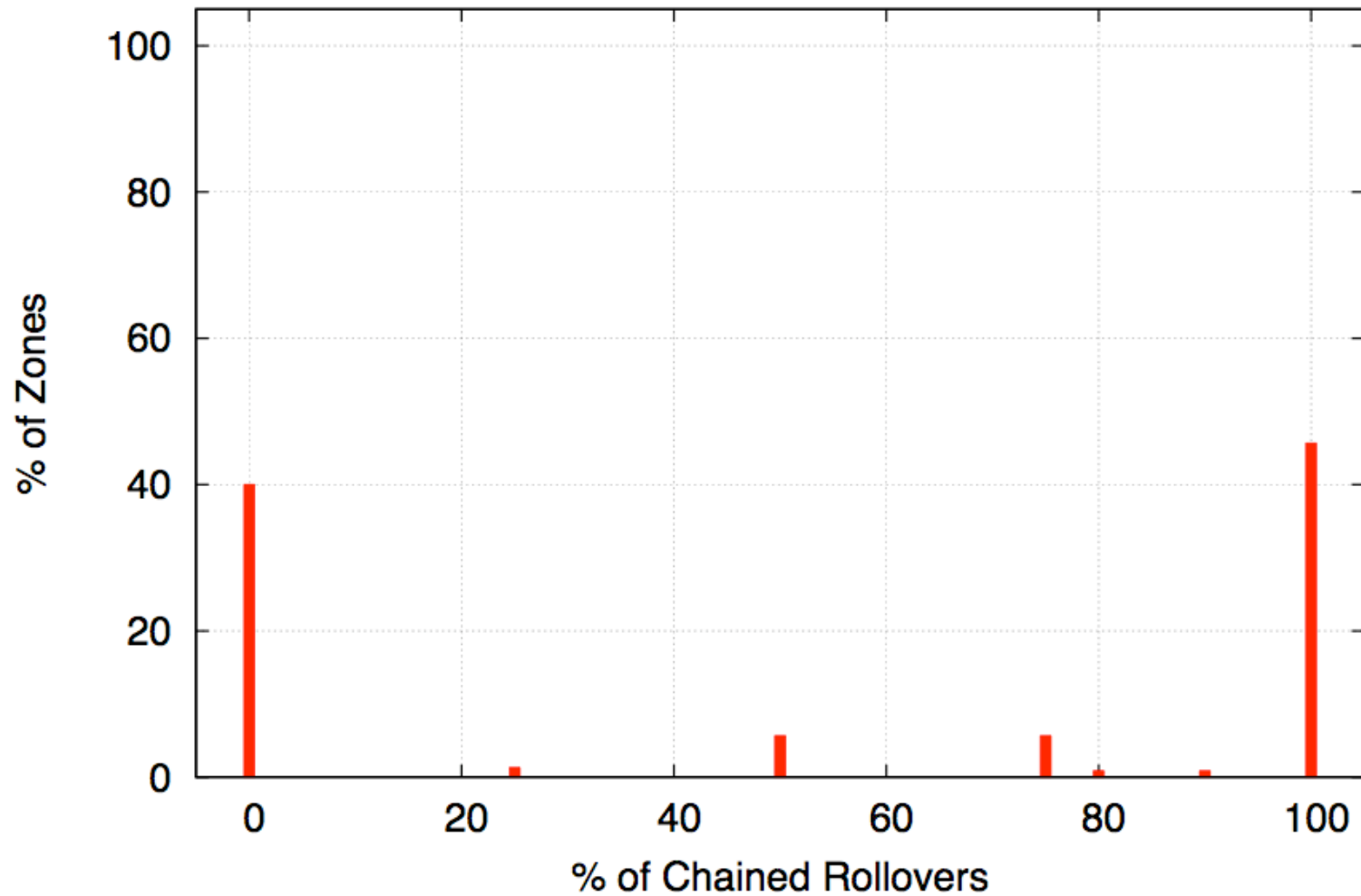
Distribution of Chained Rollovers

Distribution of Chained Rollovers



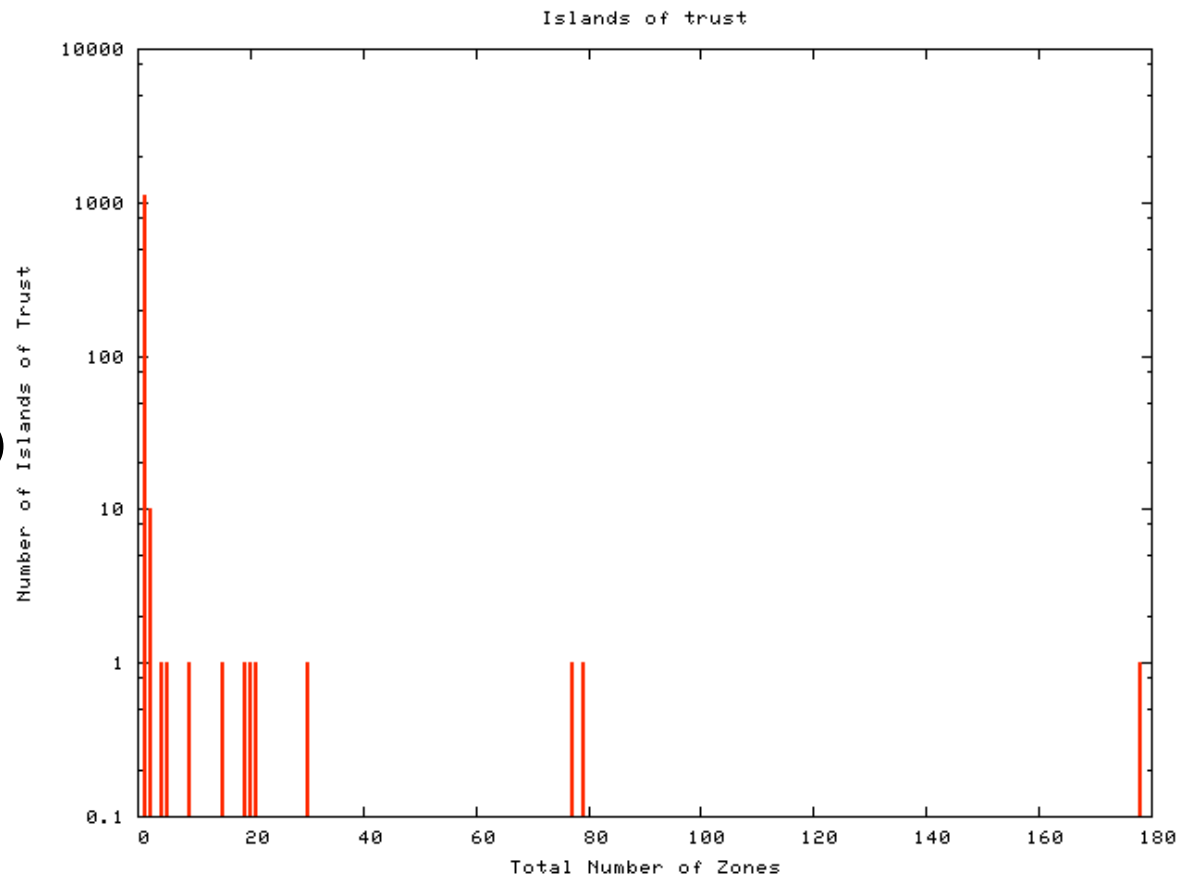
Rollovers - New Keys Only

Distribution of Chained Rollovers

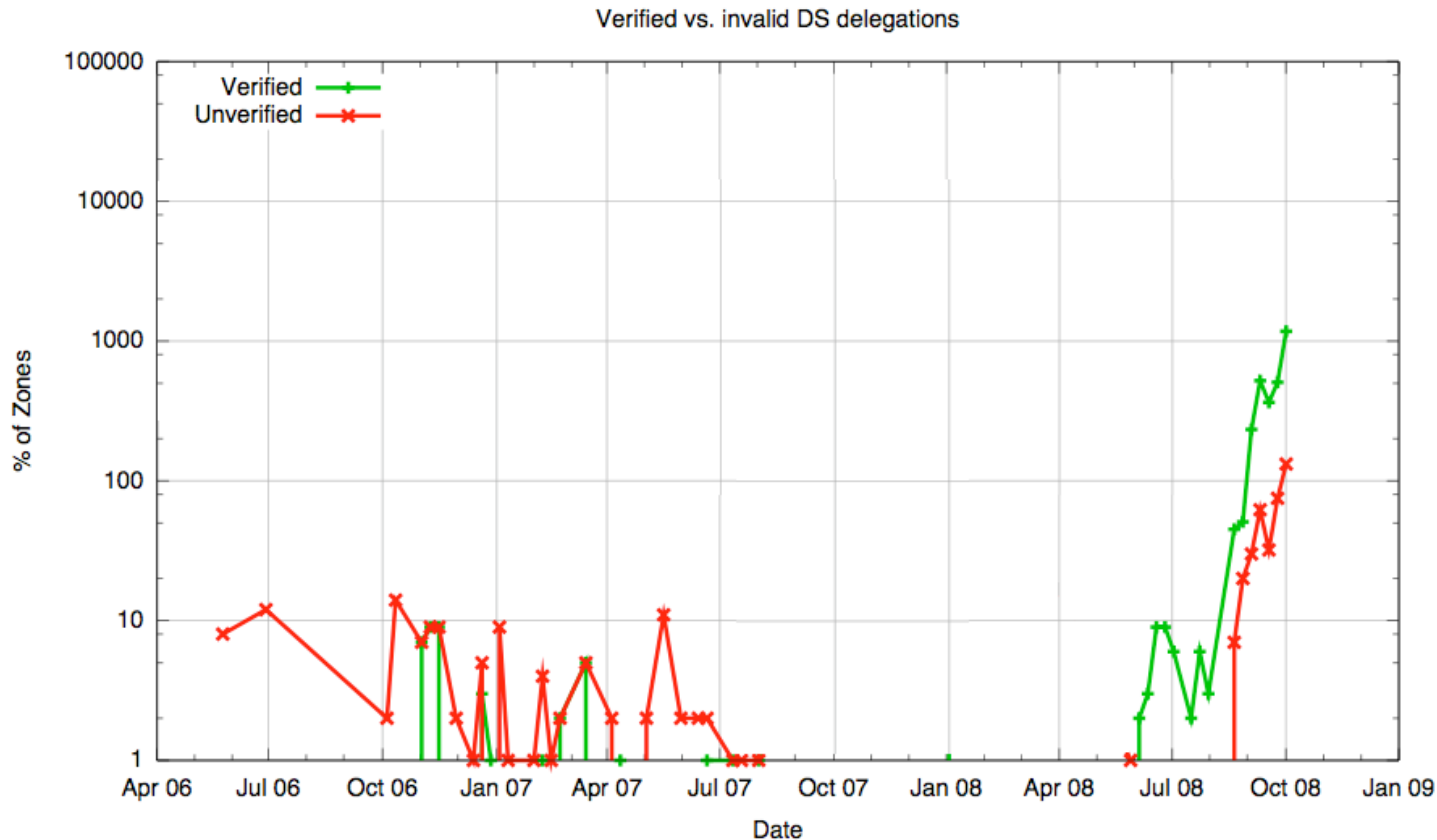


Learning Keys - the Delegation Hierarchy

- 1,134 trust anchors *today*
 - Out of 1,627 zones
 - 1,113 islands size 1 (98.15%)
- Coordination with a parent zone is an involved process



Verifiable Secure Delegations



- Monitoring blip in the middle, but w/ the uptake in DNSSEC we are seeing more misconfigurations

Conclusions

- DNSSEC is taking off
 - Though it still has a ways to go
- Though the uptake is encouraging, we must be mindful of configuration complexity / errors
- We need tools that can see misconfigurations and help operators (like SecSpider)
- We also need tools to help automate as much of the operational complexity as is safe
 - The delegation hierarchy serves as evidence that complexity can lead to slow uptake and errors


Come Visit us



SecSpider the DNSSEC Monitoring Project



[Home](#) | [Blog](#) | [About](#) | [FAQ](#) | [Documentation](#) | [Usage](#) | [Pollers](#) | [GPG Key](#) | [IRL](#)

 Check out our [blog](#)

To add a zone for monitoring, please submit below:

Zone to add:

Search for zone:

Zone:

[Vouch for or against a zone's production status](#)

<http://secspider.cs.ucla.edu/>

Questions?

Backup

Distributed Polling

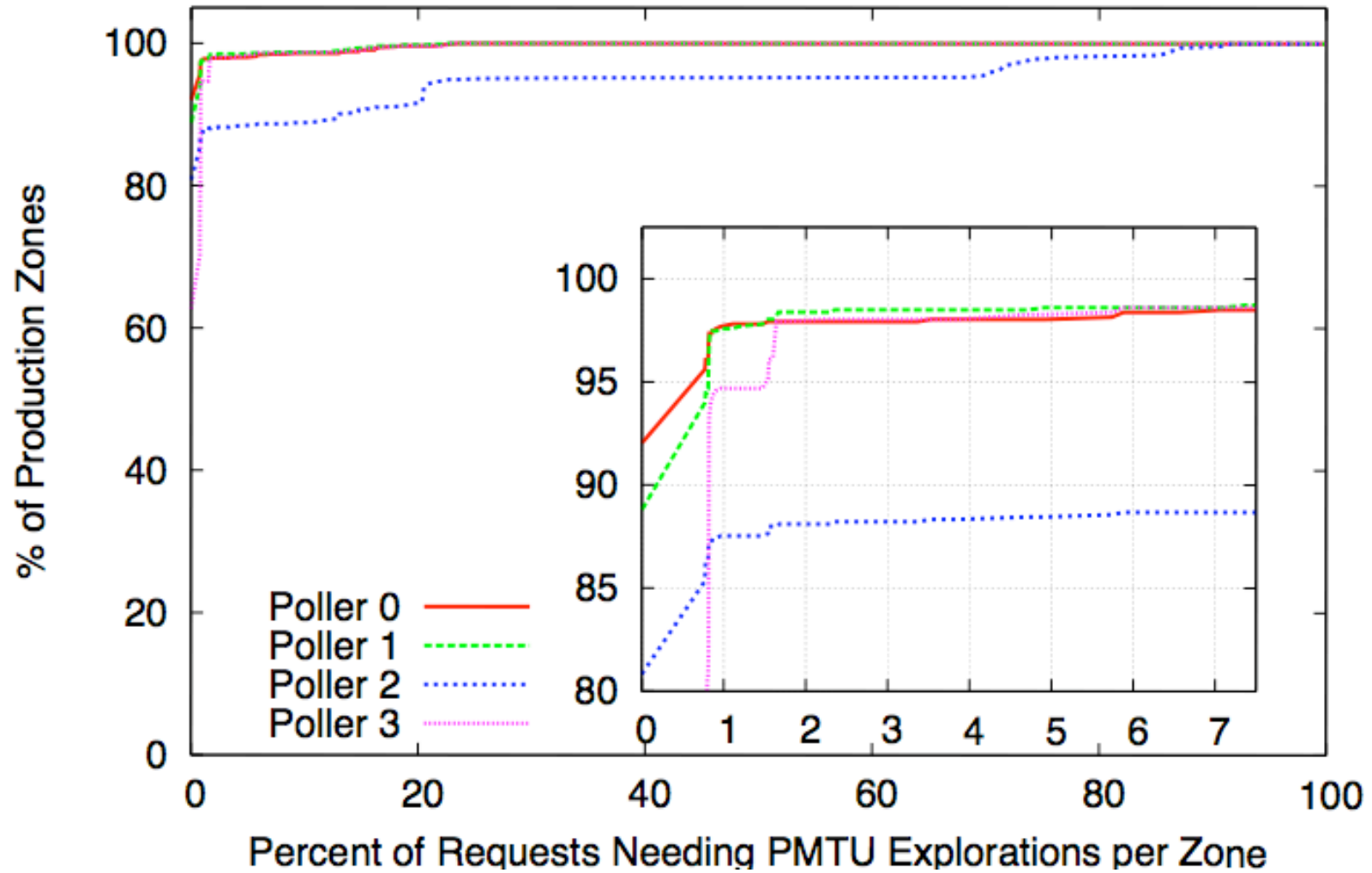
- We use distributed pollers to measure consistency (or inconsistencies)
- For example: DNSKEY RRsets spoofing at one poller will not fool others, and discrepancies can be seen
- In addition, network issues can cause some vantage points to be unable (or less able) to access DNSSEC information
 - We call this *availability dispersion*



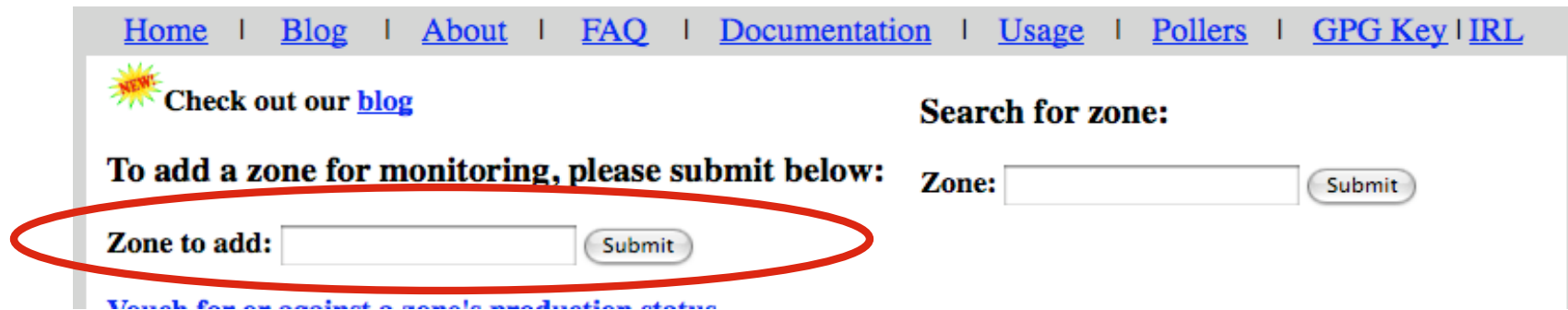
Submissions by TLD Since August 2008

- 290 ru
- 147 br
- 71 arpa
- 43 com
- 31 de
- 28 se
- 27 org
- 15 net
- 12 pr
- 11 bg
- 10 eu
- 9 fr
- 8 edu
- 8 asia
- 7 uk
- 6 hk
- 4 ch
- 3 info
- 3 gov

CDF of PMTU Explorations per Zone



How to Use SecSpider



The screenshot shows the top navigation bar with links: [Home](#) | [Blog](#) | [About](#) | [FAQ](#) | [Documentation](#) | [Usage](#) | [Pollers](#) | [GPG Key](#) | [IRL](#). Below the navigation bar, there is a section with a sun icon and the text "Check out our [blog](#)". To the right, there is a "Search for zone:" section with a "Zone:" label, an input field, and a "Submit" button. Below this, there is a section titled "To add a zone for monitoring, please submit below:" with a "Zone to add:" label, an input field, and a "Submit" button. The "Zone to add:" input field and its "Submit" button are circled in red.

- From our front page, submit your zone
- After the next polling cycle, you will see your zone on our web site
- For DNSKEYs (for example) check their consistency

Checkout Our Paper in IMC

- “Quantifying the Operational Status of the DNSSEC Deployment”

<http://irl.cs.ucla.edu/papers/imc71-osterweil.pdf>