INSIGHTS FOR THE ROAD AHEAD FROM ~20 YEARS OF DNSSEC RESEARCH

Eric Osterweil

eoster@gmu.edu

Assistant Professor

Department of Computer Science, George Mason University

GEORGE MASON UNIVERSITY

WHY STUDY SOMETHING (DNSSEC) FOR ~20 YEARS?

- Studying large scale deployments of protocols over the long term can yield a variety of results
- Sometimes protocols have unforeseen problems
- And sometimes they have unforeseen benefits
- In its first ~2 decades, DNSSEC has shown both

- In my experience, this long-term research requires persistence
  - (or stubbornness, it depends on the results)
  - Conscientious system-building can enable deep science (especially over time)

``… monitoring and debugging is a detailed and tedious thing, but I believe there is some deep science one can find in the process…'' – Lixia Zhang '05

EVOLUTION OF DNSSEC'S LESSONS

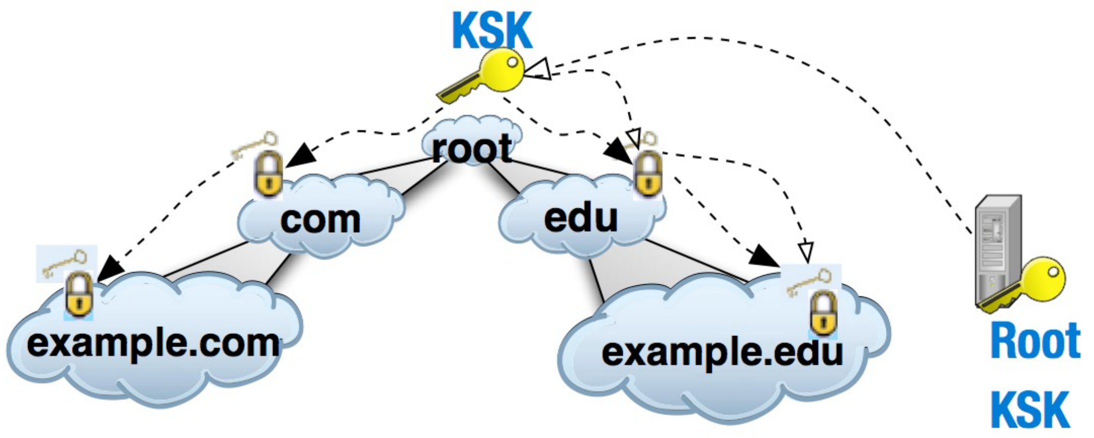
- Opinion: DNSSEC has offered opportunity to learn rare lessons about security operations at scale
- In particular, DNSSEC's research value proposition has evolved during its lifetime
  - At the beginning of this a first-of-its-kind security deployment, we studied how well it was working
  - As it has matured, we have the opportunity to learn from it and discover basic principles of security at scale!
- Findings have ranged from:
  - Anecdotal – Such as deployment incentive necessities
  - To pervasive – Like design choices that reduce attack surface
  - To security invariants – i.e., Lifecycle management for long term security of objects
- With the rise of security for digital objects, I believe DNSSEC may provide key insights needed for future object-security protocols

OUTLINE

- A brief DNSSEC primer
- Some challenges that have faced DNSSEC in ~20 years of deployment
- Evolution of findings
- Discussion and futures

A BRIEF DNSSEC PRIMER

- First attempt to secure a core Internet protocol w/ crypto



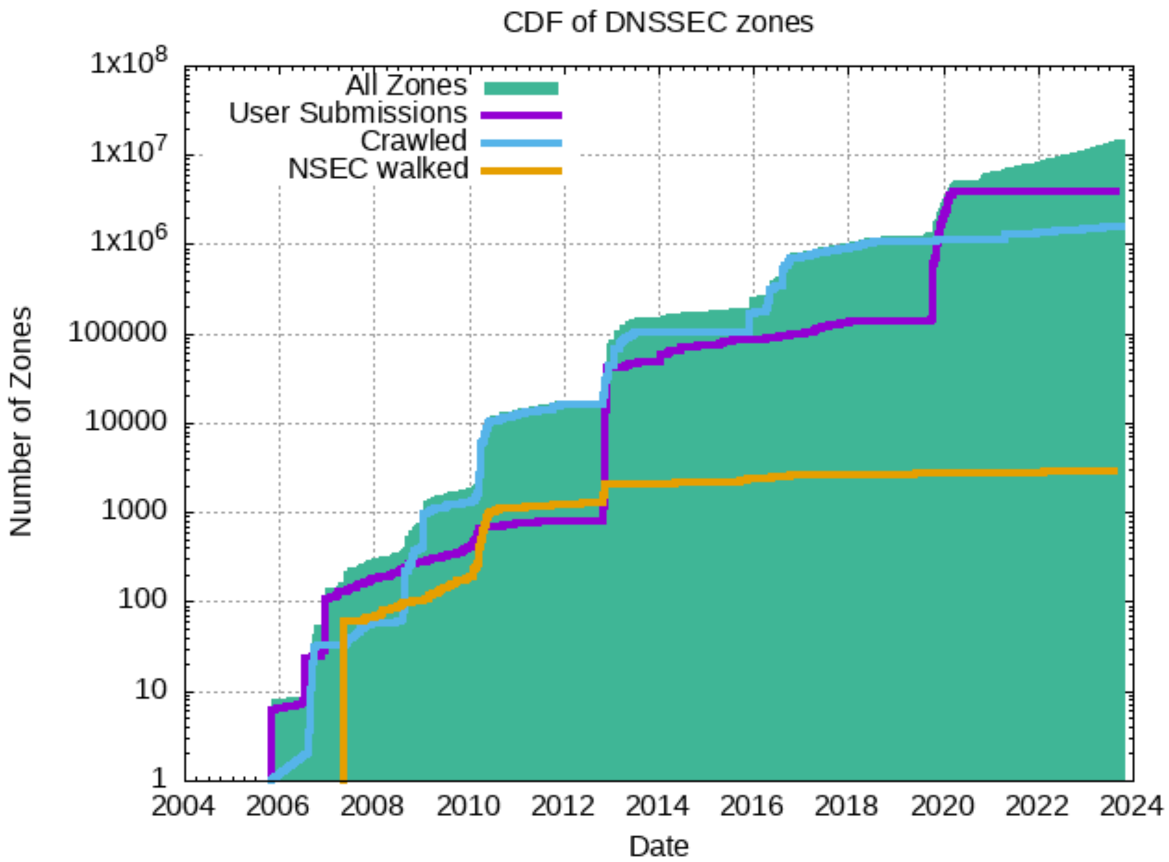
- DNSSEC zones create pub/priv keys
  - Public key is DNSKEY

- Zones sign all RRsets and resolvers use DNSKEYs to verify them
  - Each RRset has a signature attached to it: RRSIG

- Resolvers are configured with a *single root* key, and *all* trust flows recursively down the hierarchy

FUNDAMENTALLY

- DNSSEC is a relatively simple design
  - Hierarchical cryptographic key learning system
- However, it was the first of its kind
  - First time a core Internet protocol was cryptographically enhanced
  - Upgraded in place
- Now almost 14 million zones worldwide



https://secspider.net/

A RESEARCH PERSPECTIVE

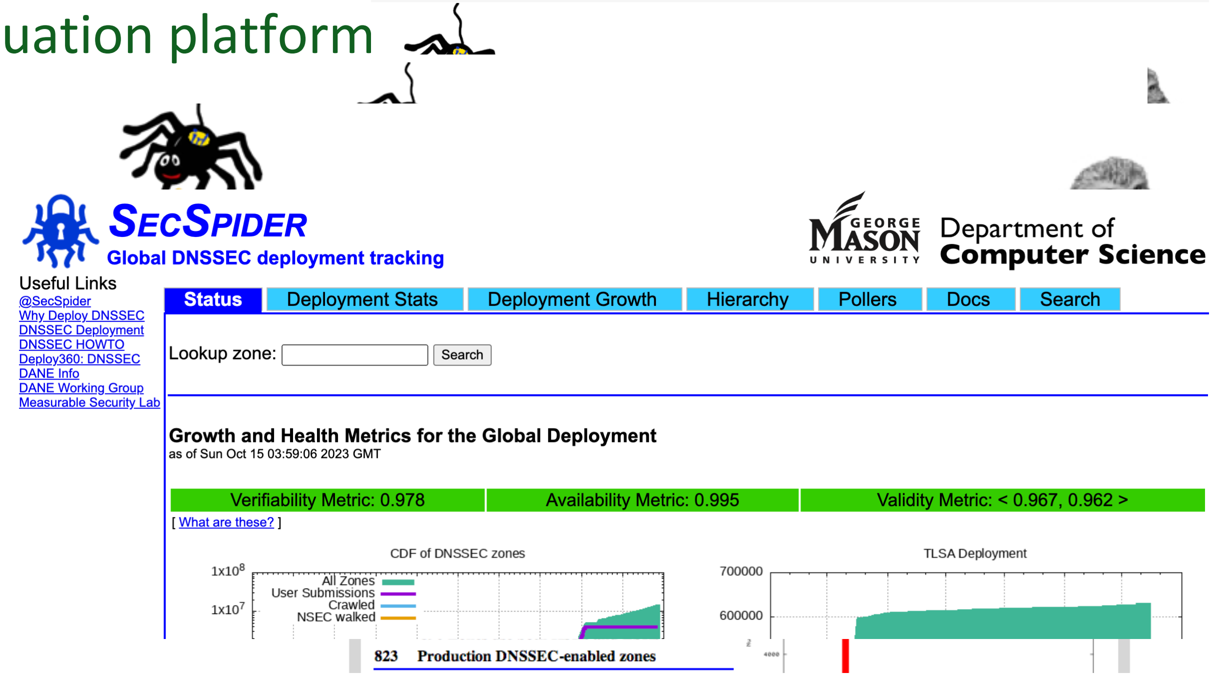
- DNSSEC has, essentially, been a big experiment
  - Can we upgrade a live core Internet protocol with security assurances?

- Studying this first-of-its-kind security deployment from the beginning
  - A rare opportunity
  - Has given an important perspective

- The deployment of security at this scale, for this duration has allowed us to learn valuable lessons
  - What has it taught us?
  - Where can we apply those lessons/findings?
  - What was expected, and unexpected?

SYSTEMS BUILDING TO FACILITATE RESEARCH

- Early on, (in 2005) we developed an evaluation platform SecSpider https://secspider.net/



- Over the years, it evolved:
  - Was rewritten three times
  - Has had two database schemas
  - It suffered from outages
  - But it has endured and grown
  - Now has roughly 54 billion records in its database
  - Developing, evolving, and maintaining this system and dataset was a nontrivial result

- Fundamentally, it has preserved an archive of how this experiment (DNSSEC) performed
- This has given us an ongoing/quantitative view into what DNSSEC's global deployment is/was facing

DNSSEC'S CHALLENGES

FORESEEN CHALLENGES DNSSEC FACED

- Designers proactively considered the incremental rollout DNS → DNSSEC would face
- Hierarchical keys would, necessarily, not start from the root: ``Islands of security''
- When crypto did come to the root, it was a Deliberately Unvalidatable Root Zone (DURZ)
- Literally:

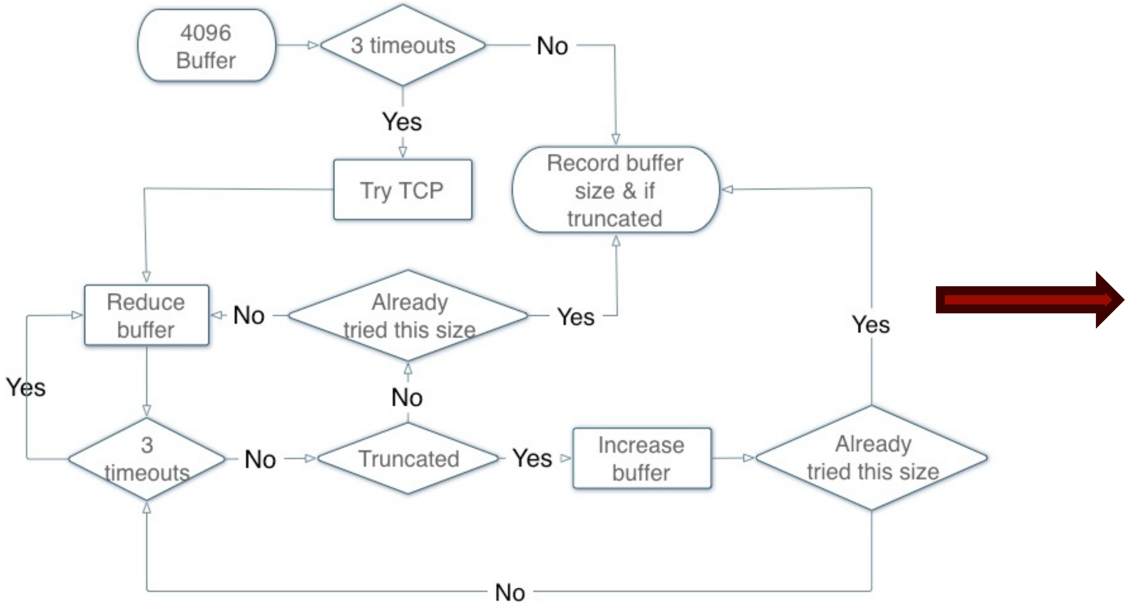
AwEAAa2Yy++++++++++++++++
THIS/IS/AN/INVALID/KEY/AND/S
HOULD/NOT/BE/USED/CONTAC
T/ROOTSIGN/AT/ICANN/DOT/OR
G/FOR/MORE/INFORMATION++
++++++++++++++++++++++++++
++++++++++++++++++++++8

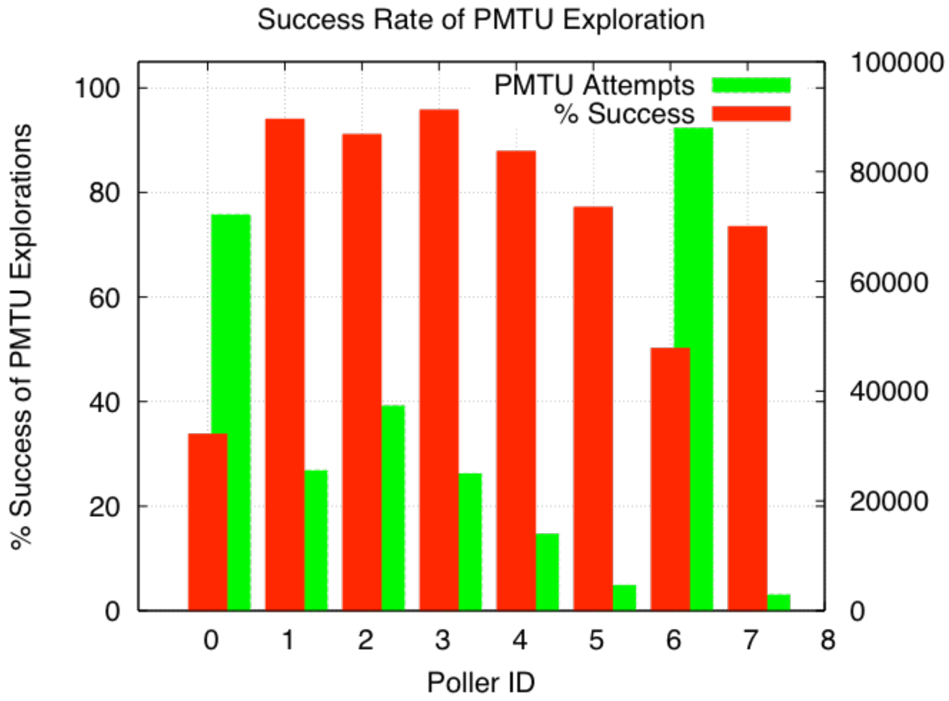
UNFORESEEN CHALLENGES FACED

- As is common in many operational systems, unforeseen problems have come and gone
- One prominent example was the discovery of "***Availability***" problems
  - i.e., Path Maximum Transmission Unit (PMTU) failures
- Was due to all of the extra data DNSSEC added to DNS packets
  - We added multiple crypto keys (DNSKEYs), anywhere up to 4,096 bits each
  - We added crypto signatures (RRSIGs)
  - Resolvers and name servers need to send and receive these large DNS packets
- DNS messages were further limited by "middle boxes" (firewalls, NAT, etc.)
  - Some firewalls drop "suspicious" DNS traffic
  - A study, at the time, found this was quite common in SOHO routers

PMTU EVALUATION

- After discovering this unexpected failure mode, we evaluated [1]





- Green bars indicate the number of times a poller needed to do a PMTU walk
- Red bars indicate the percentage of times a PMTU was was able to find a buffer size the allowed DNSKEYs to be received
- Which led to reduced occurrences

[1] Osterweil, Eric, Michael Ryan, Dan Massey, and Lixia Zhang. "Quantifying the operational status of the dnssec deployment." In *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, pp. 231-242. 2008.

ATTACKS FACED

- More unforeseen: system has endured attacks and encroachment

- DNS cache poisoning was a known attack since the 1990s [2], but then came the "summer of fear" in 2008 (i.e., the Kaminsky attack)
  - Cache poisoning became possible from off-path attackers

- In 2017, the DNSpionage attack affected DNS
  - Overcame DNSSEC by disabling it

- Most recently, blockchain-based name systems/services
  - Have begun to rediscover the complexities of Internet naming under the premise that control of DNS/DNSSEC is centralized in nature

[2] Bellovin, S. M. 1995. Using the domain name system for system break-ins. USENIX UNIX Security Symposium 1995

LESSONS AND DERIVED BENEFITS

- Deeper lessons and derived benefits have been found from unexpected directions

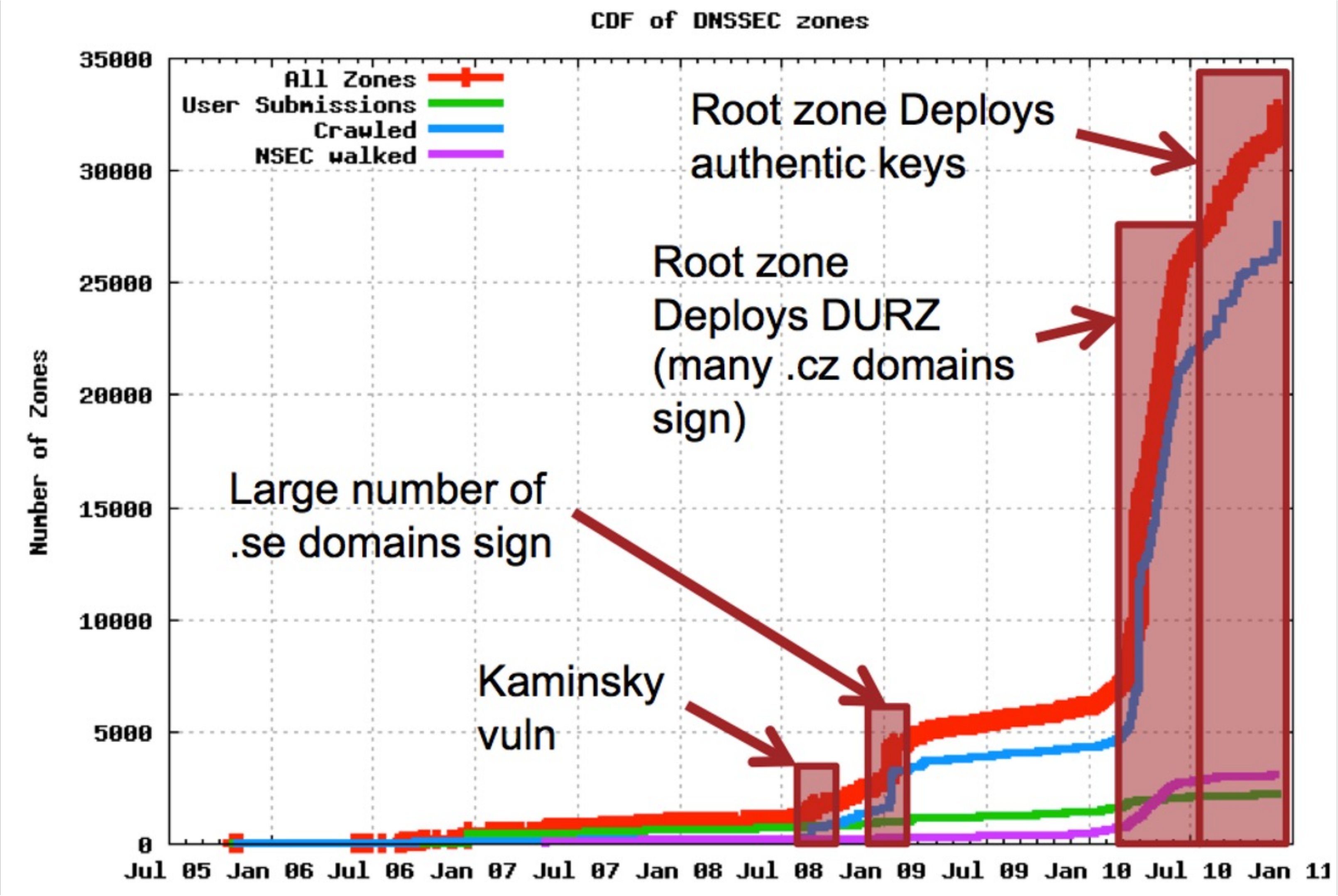
- A few key examples
  - Having an ``incentive model'' has proven to be an important (necessary?) precondition
  - Design choice of enabling ``offline keys'' → Reduced attack surface
  - Open governance → More distributed than most realize
  - Caching and key lifecycle management → object-security properties

``IF YOU BUILD [WHO] WILL COME[?]''

- Since the beginning we have not clearly explained ``why do DNSSEC?''
  - Enhancing, even a core Internet protocol, with security does not necessarily get it deployed
- Especially at the beginning, there were struggles to spur deployment
- Lots of challenges and lots of risk
- Back then, the tools were not very helpful
  - Today, is better, but the question remains
- Real operations are run by businesses, the value proposition is important

https://www.smh.com.au/sport/it-s-perfect-costner-s-scene-stealer-as-baseball-emerges-into-a-field-of-dreams-20210813-p58ihh.html
Field of Dreams (1989)

INCENTIVIZING DEPLOYMENT MATTERS



ALSO SOME MUCH LESS OBVIOUS LESSONS: OFFLINE KEYS

- DNSSEC has a simple design requirement:
  be able to keep private keys offline while zones operate

- This was done to reduce vulnerability of private keys
  - If an adversary breaks into a server, she cannot then learn private keys
- Resulted in some extra design complexity of DNSSEC
  - Proving non-existence in advance (i.e., NSEC/NSEC3 records), etc.

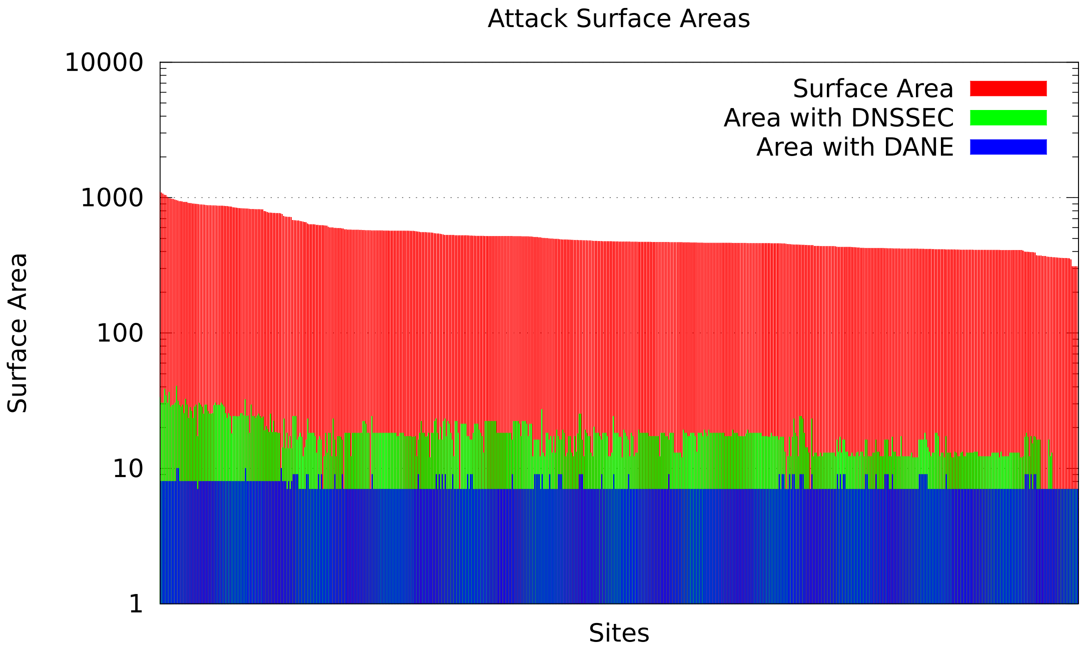
- However, resulted in an important ramification
  - DNSSEC servers (i.e., secondary name servers) ***cannot*** lie
- For illustration, consider other network security protocols, like TLS, BGPSec, etc.
- It turns out to be rare to find a protocol where endpoints can be *untrusted*
- DNSSEC created that

REDUCED ATTACK SURFACE

- To evaluate, cast this in terms of ``attack surface’’

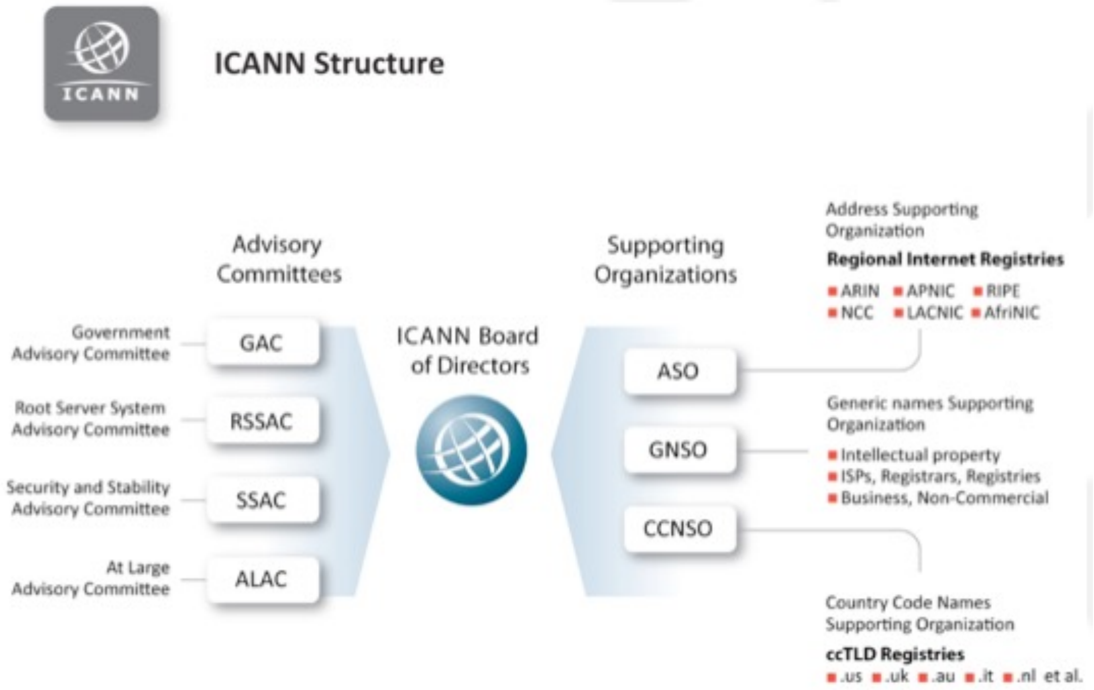
- The basic advance this enables is data objects are protected at their source, even while ``at rest’’ on their own servers

- [3] Osterweil, Eric, Danny McPherson, and Lixia Zhang. "The shape and size of threats: Defining a networked system's attack surface." In 2014 IEEE 22nd International Conference on Network Protocols, pp. 636-641. IEEE, 2014.



OPEN GOVERNANCE

- Trust in the DNSSEC begins with trust in its root
- In DNSSEC, the Root zone is just one step, and its duties are not centralized, compartmentalized
- Ultimately, you don't trust the Root of DNSSEC, you trust its Multi-Stakeholder Community
  - What goes into the Root: ICANN multi-stakeholder community
  - Who "manages" the contents: ICANN Org
  - Who "maintains" and operates the official contents: VeriSign, Inc.
  - Who operates servers: Root Server Operators (RSOs), 12 of them
- There is no single party to "trust," the process is open and community-driven: very distributed



https://gnso.icann.org/sites/default/files/filefield_34765/presentation-multi-stakeholder-model-14oct12-en.pdf

CRYPTO KEY MANAGEMENT

- In the early days, everything was manual
  - Keying
  - Creating/managing secure delegations
  - Key rollovers/transitions
  - …

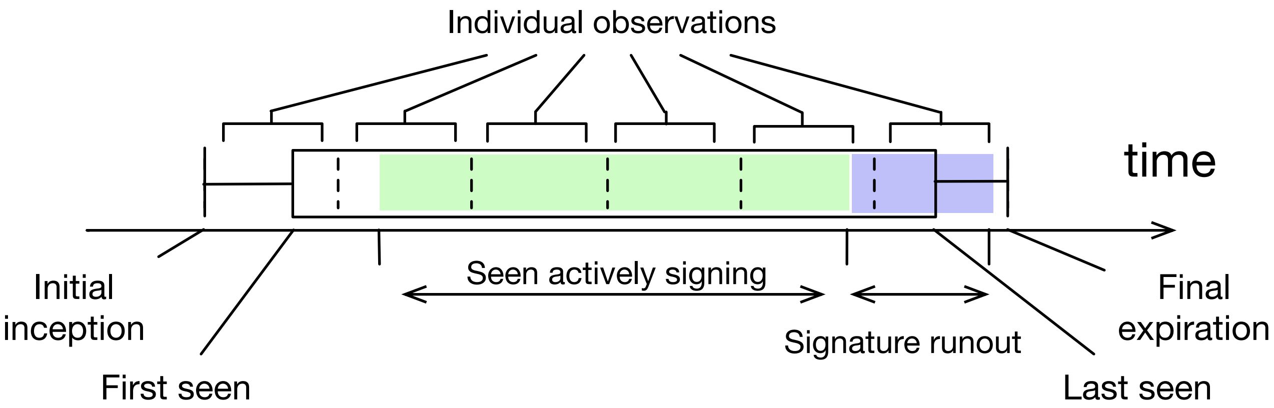
- Early on, keys were largely static (or very long-lived), and the rate of change, and rules for managing their lifecycles, were largely absent

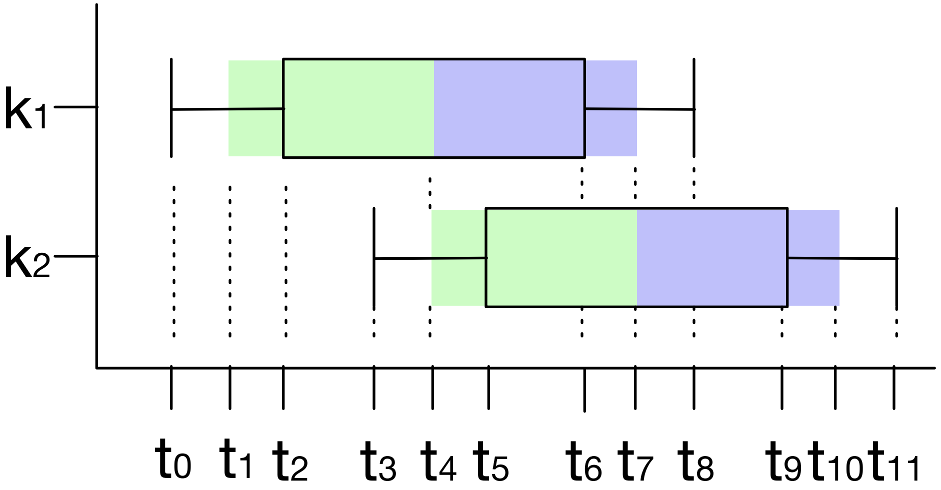
- Has been fascinating to use a data-driven approach to quantitatively evaluate the effects of developing ``wisdom'' (i.e., standards)

- The road to evaluation has proven, at times, to be a long one

EVALUATING KEY MANAGEMENT FROM LONGITUDINAL MONITORING

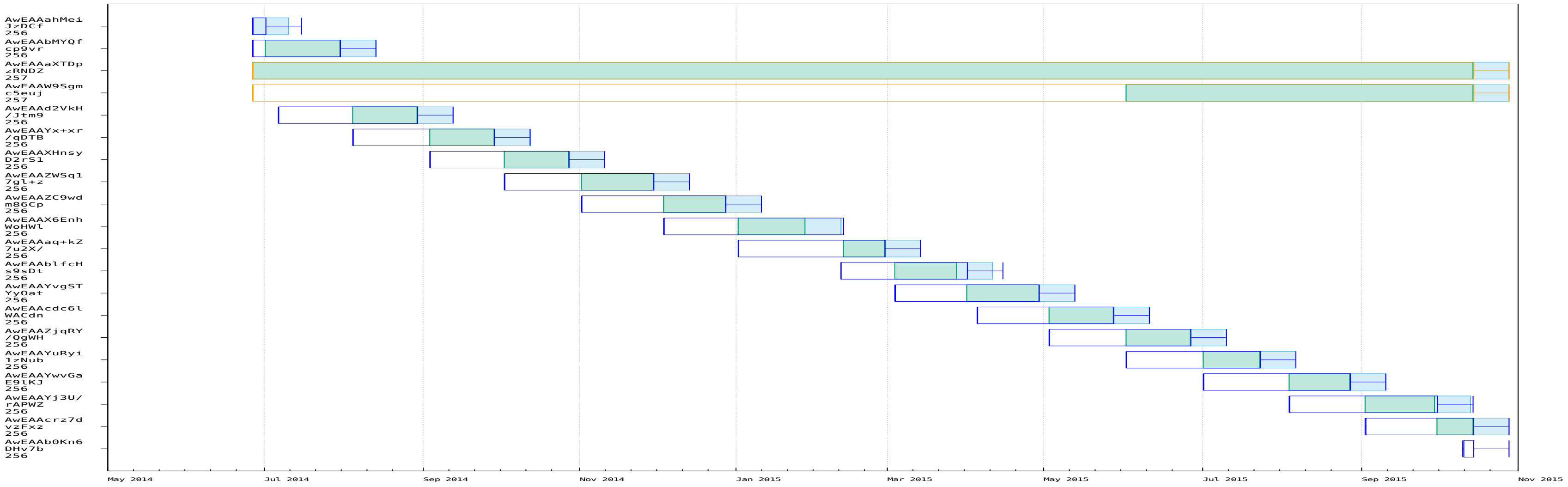
- There is no quantitative way to see or verify if this is being done correctly (securely)
- But, active measurements of the global infrastructure only let us see one snapshot at a time
- Longitudinal behaviors like key lifecycle management are timeseries
  - So, what do key rollovers actually look like, and are they "working?"
- We start from conscientious monitoring and measurement, then we model and analyze phenomena
- As photo snapshots can be projected into video, measurements must become models
- Bridged and Busted observations are the Bound into longitudinal key entities

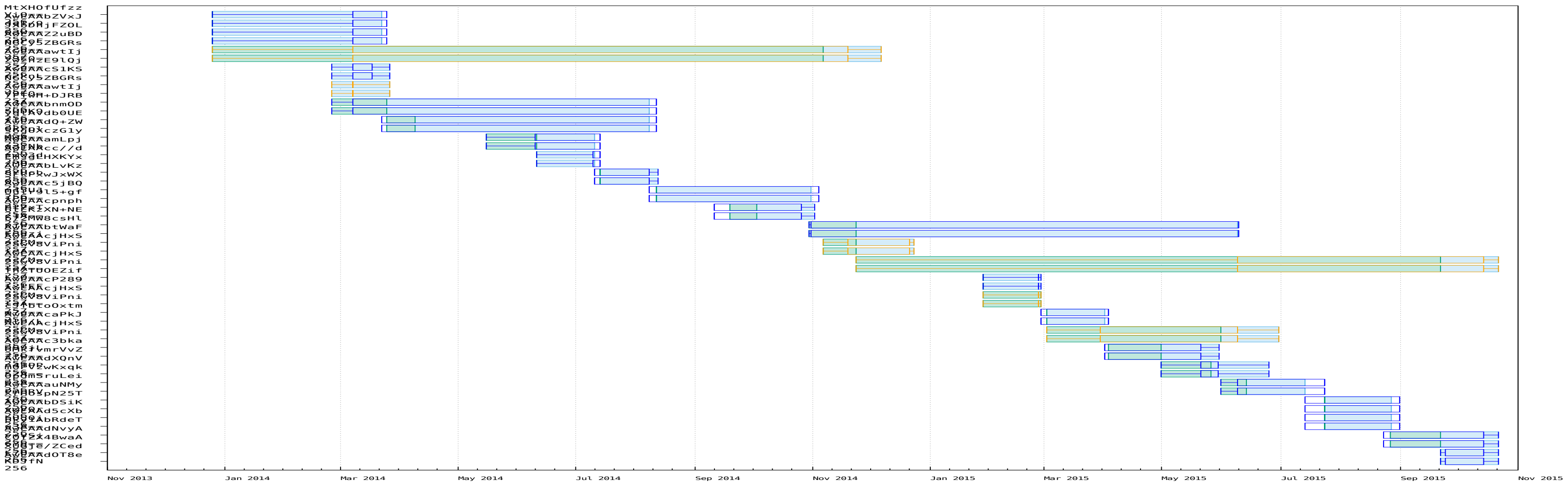




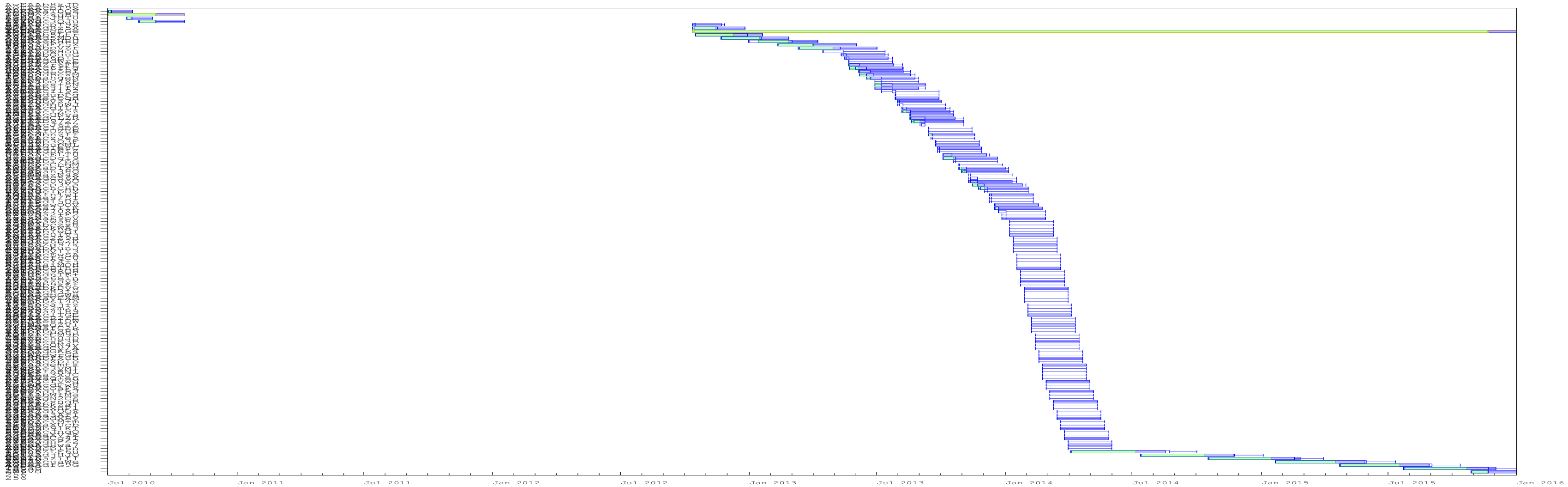
[4] Osterweil, Eric, Pouyan Fotouhi Tehrani, Thomas C. Schmidt, and Matthias Wählisch. "From the beginning: Key transitions in the first 15 years of DNSSEC." *IEEE Transactions on Network and Service Management* 19, no. 4 (2022): 5265-5283.

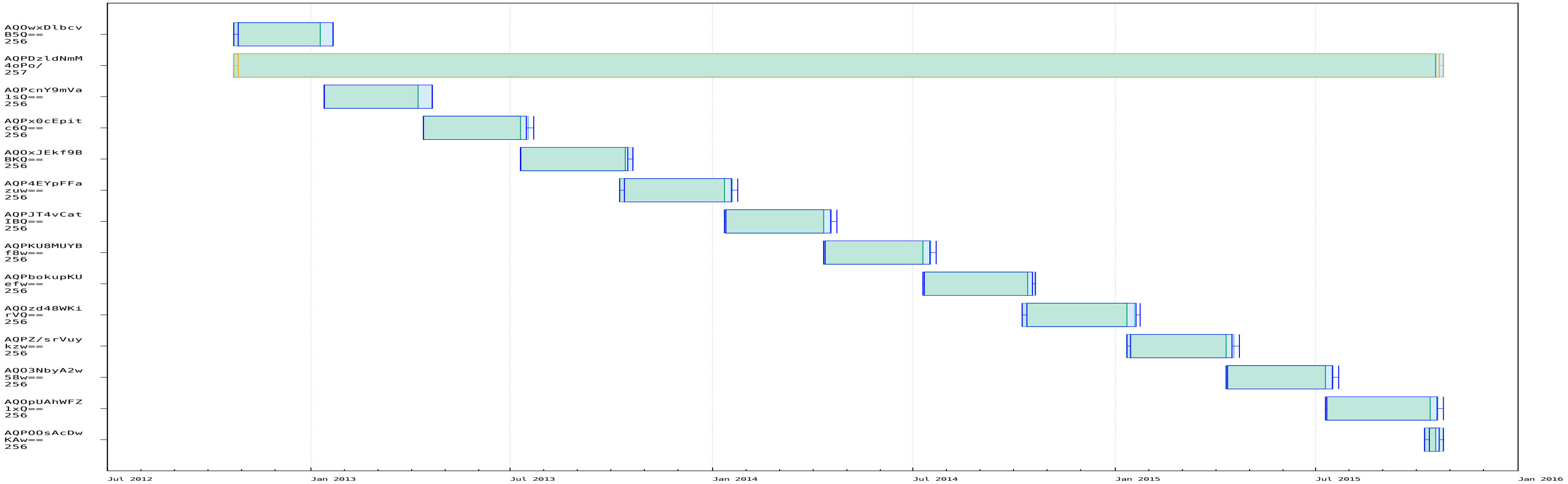
A NOVEL VISUALIZATION OF KEY LIFECYCLES IN PRODUCTION ZONES





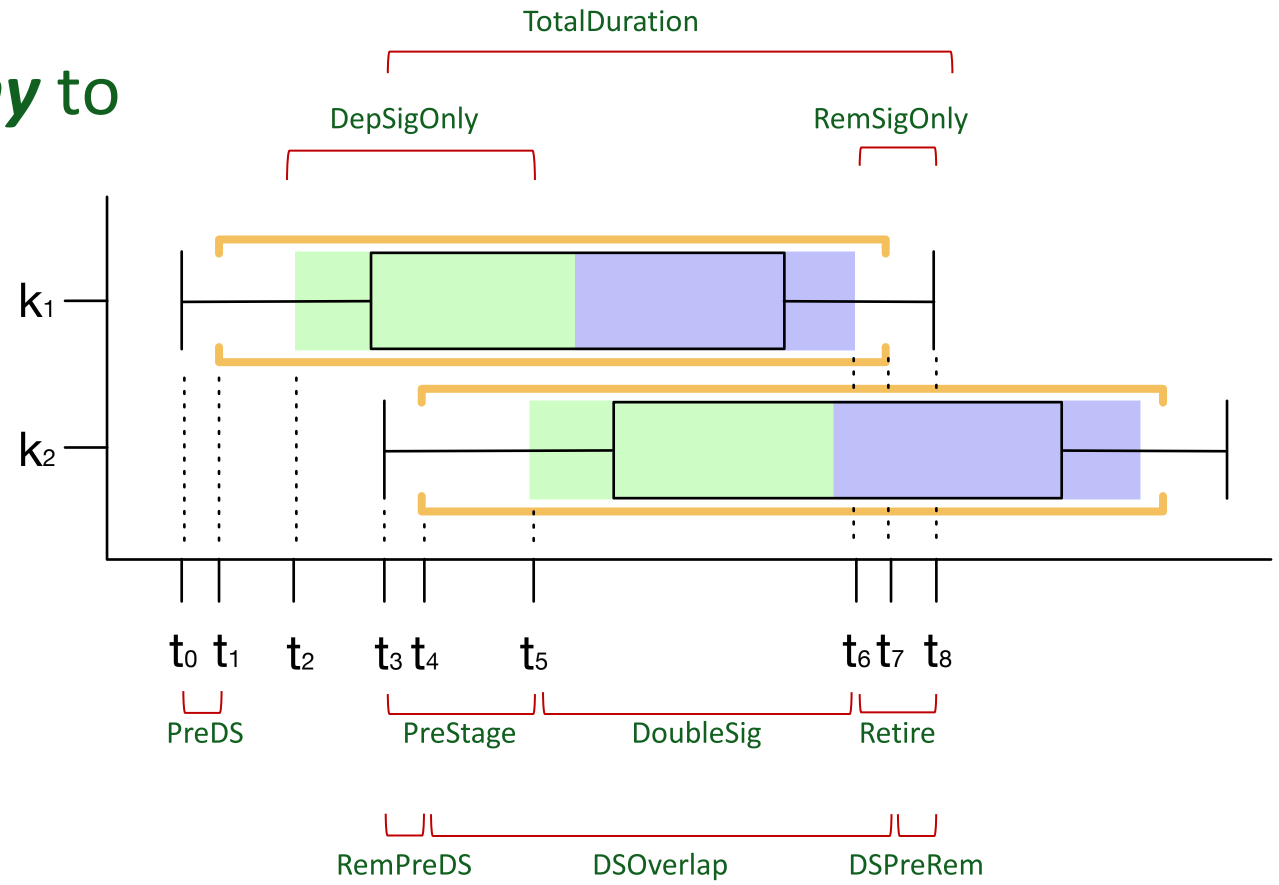
QUANTITATIVELY DIFFERENT BEHAVIORS





EVALUATION: AN ANATOMY OF A KEY TRANSITION

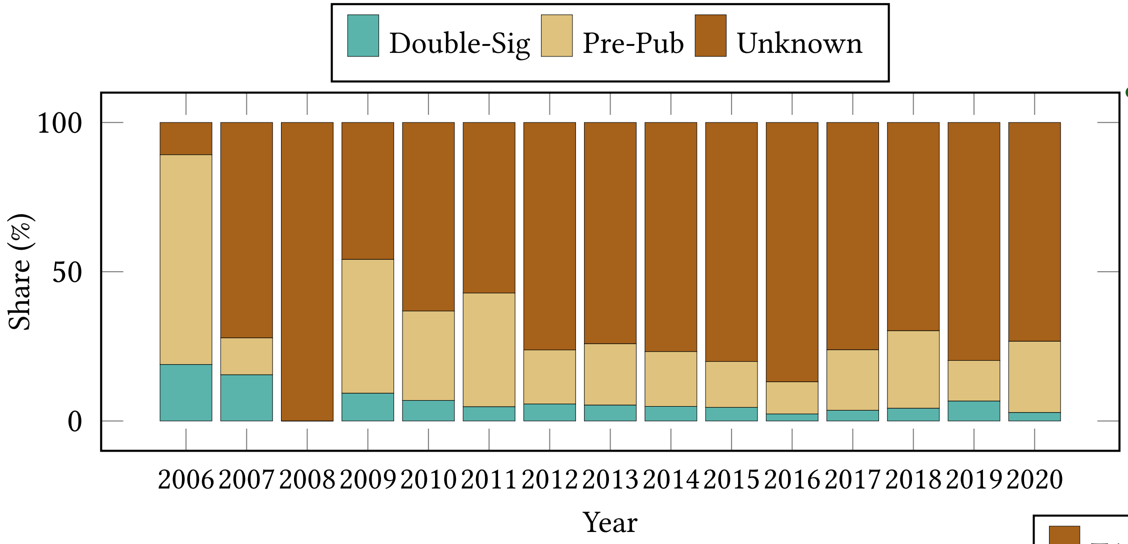
- A key transition ***anatomy*** to map the topography
  - Use RFCs as ***hypotheses***
  - Then we can *test* these hypotheses



	PreDS	*DoubleSig*	*PreStage*	*DepSigOnly*	*Retire*	*DSOverlap*	*RemSigOnly*	*DSPreRem*	*RemPreDS*
ZSK Pre-Pub		$= 0$	> 0 M	> 0	> 0		> 0		
ZSK Double-Sig		> 0 M	$= 0$ M	$= 0$	$= 0$		> 0		
KSK Double-DS	< 0	$= 0$	$= 0$	$= 0$	$= 0$	> 0 M	> 0	< 0 M	< 0 M
KSK Double-KSK	> 0	> 0	$= 0$	$= 0$	> 0	$= 0$	> 0	> 0 M	> 0 M
KSK Double-RRset	> 0	> 0	$= 0$	$= 0$	> 0	$= 0$	> 0	$\neq 0$ M	

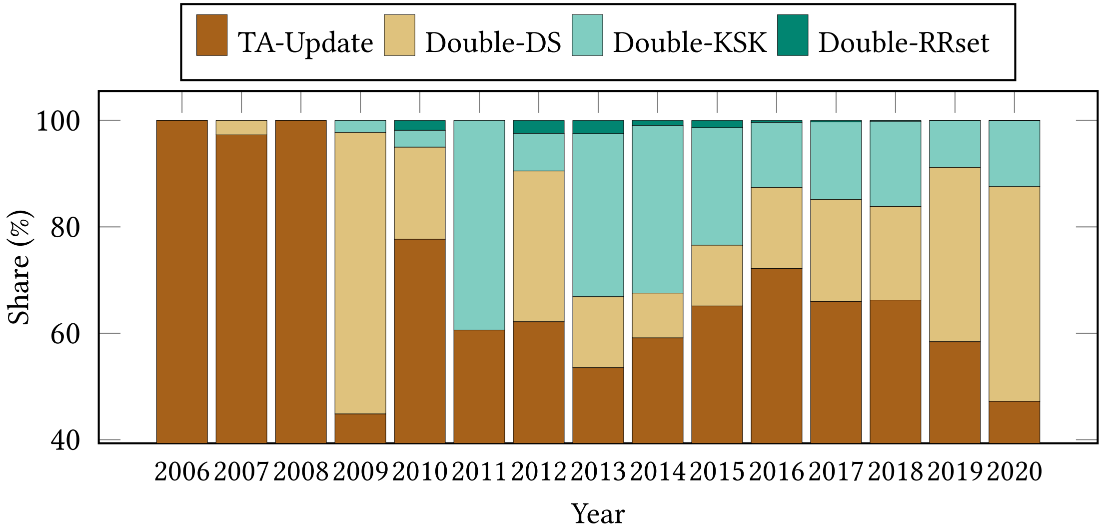
MEASURING AGAINST THE KEY TRANSITION ANATOMY

- We measured which (if any) RFC key transition process zones followed



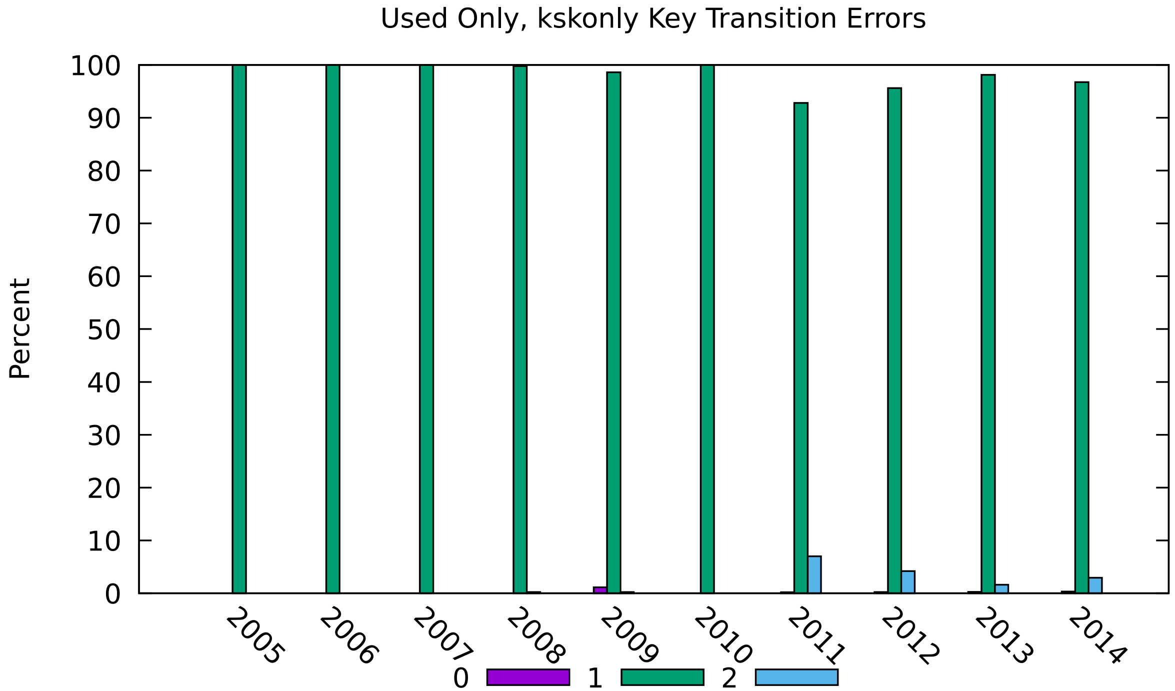
- Most ZSKs followed non-standard ZSK transitions

- For KSKs, all RFC-5011 compliant until the DNSSEC chain-of-trust started to develop (~2008)
- There was much more heterogeneity for KSKs



KSK ERRORS AND WARNINGS

- For KSKs, almost all rollovers were at least in a warning state
  - 0== no error, 1 == warning, and 2 == error
- Deviations from RFC guidance doesn't *necessarily* mean an error
  - For KSKs, only violations at affect the ***correctness*** of a transition constitute "error"



THE BIGGER PICTURE, UNEXPECTED RESULTS

- DNSSEC has, indeed, taught us a lot!
- Some very interesting properties of DNSSEC come from its longitudinal protections of DNS' data *as objects*
- DNSSEC's research results may illustrate an unexpected security model: loosely referred to as ``object-security''

- The picture becomes more expressive and clearer with increasing resolution
  - Incentive model
  - Reduced attack surface, because DNSSEC manages ***objects***
  - A much more distributed substrate (from the root down) than most realize
  - Caching and key lifecycle management have illustrated object-security properties

- Results suggest that DNSSEC is perhaps one of the first protocols to operationalize critical preconditions for a type of protections of ``object-security''

ONGOING / FUTURE WORK

- Developing an understanding of, and definition for, precisely what ``object-security'' means

- Conscientious monitoring and evaluation of DNSSEC's trials and tribulations reveal basic natures of how ***it*** secures objects at scale

- Other protocols have established protections over digital objects, but
  - Have they been operationally successful, and why/why not?
  - Should they be classified as object-security protocols, or not?

- We are considering what other protocols and systems have effectuated object-security protections and what should an Internet service model look like for object-security, and why

THANK YOU!

QUESTIONS?
EOSTER@GMU.EDU

BACKUP