Digital Signatures

- Used to proof authenticity
- Alternative use of a public key cryptosystem
  - e.g., RSA
- Exchange encryption/decryption steps
  - Often used on a message digest
- More details to come …

1

Domain Name System (DNS)

- Map
  - Human memorable hostname
    e.g.: www.net.in.tum.de
  - Machine usable addresses
    e.g.: 131.159.15.242
- DNS system
  - Application vital to the Internet
  - Transparent to the user
  - Distributed, hierarchical, redundant
  - Uses caching

2

Need for "secure" DNS

- DNS: no mechanism for authentication
- 1990's real world attacks:
  - Show how easy misuse of DNS is
  - Attacks:
    - Spoofing
    - Sniffing + answer injection
    - Guessing and predicting query Ids
    - Cache poisoning
  - Bellovin Usenix95:
    "Using the Domain Name System for System BreakIns"
  - Vixie: Usenix95:
    "DNS and BIND Security Issues"

3

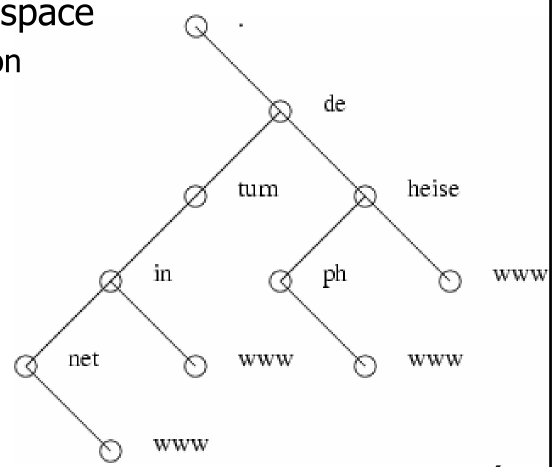
DNSSEC: "secure" version of DNS

- Developed over the last 10 years
- Goals:
  - full backward compatibility
  - Data integrity
  - Data authenticity
- Problems:
  - Overhead???
    - Bandwidth
    - Resource consumption: Memory, CPU
  - Deployment issues
    - Key management (PKI)
    - Configuration

4

DNS

- ❒ Distributed database
- ❒ Hierarchical name space
  - ❍ Based on delegation of responsibility



5

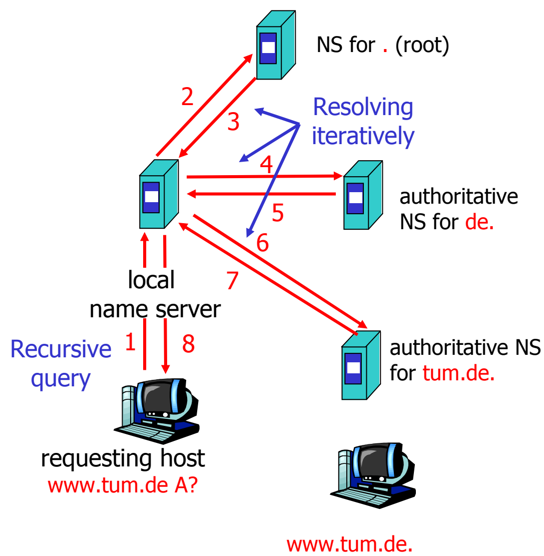
DNS protocol

- ❒ Query ↔ Response (1-to-1 relationship)
- ❒ UDP (TCP as fallback)
- ❒ DNS message
  - ❍ Four sections
    - Query
    - Answer
    - Authority
    - Additional
- ❒ Resolution process
  - ❍ Iterative
  - ❍ Recursive

6

DNS example

- ❒ Iterative queries
- ❒ Intermediate name servers
  - ❍ Delegated zones
  - ❍ Query referral
- ❒ Information
  - ❍ Resource records (RR)
  - ❍ Can be cached
- ❒ Query types
  - ❍ recursive
  - ❍ iterative



7

DNSSEC (Delegation Signer) Basics

- ❒ Idea
  - ❍ Authentication chain: root zone to resource record (RR)
  - ❍ Parent zone guarantees child zone key
- ❒ Realization
  - ❍ Four new record types
    - RRSIG signatures for resource records (RRs)
    - DNSKEY public key for the zone (e.g., RSA)
    - DS digest of the child-zone's DNSKEY (at delegation points in parent zone child's name equals DS RR's name)
    - NSEC needed for certifying non existance
  - ❍ Upward compatibility
    - Islands of security

8

Resolving with DNS/DNSSEC

- Resolving A www.tum.de.: empty resolver cache

DNS
Zone:
NS:

9

Resolving with DNS

- Resolving A www.tum.de.: empty resolver cache

DNS
Zone: .
NS: de.

10

Resolving with DNS

- Resolving A www.tum.de.: empty resolver cache

DNS

Zone:	.	de.
NS:	de.	tum.de.

11

Resolving with DNS

- Resolving A www.tum.de.: empty resolver cache

DNS

Zone:	.	de.	tum.de.
NS:	de.	tum.de.	
A:			www.tum.de

12

Resolving with DNSSEC

- Resolving A www.tum.de.: empty resolver cache

DNS/DNSSEC

Zone:	.
NS:	de.
DS:	de.
RRSIG DS:	de.

13

Resolving with DNSSEC

- Resolving A www.tum.de.: empty resolver cache

DNS/DNSSEC

Zone:	.	de.
NS:	de.	tum.de.
DS:	de.	tum.de.
RRSIG DS:	de.	tum.de.

14

Resolving with DNSSEC

- Resolving A www.tum.de.: empty resolver cache

DNS/DNSSEC

Zone:	.	de.	tum.de.
NS:	de.	tum.de.	
DS:	de.	tum.de.	
RRSIG DS:	de.	tum.de.	
RRSIG A:			www.tum.de.
DNSKEY:			tum.de.
A:			www.tum.de

15

Resolving with DNSSEC

- Resolving A www.tum.de.: empty resolver cache

DNS/DNSSEC

Zone:	.	de.	tum.de.
NS:	de.	tum.de.	
DS:	de.	tum.de.	
RRSIG DS:	de.	tum.de.	
RRSIG A:			www.tum.de.
DNSKEY:		de.	tum.de.
A:			www.tum.de

16

Resolving with DNSSEC

- Resolving A www.tum.de.: empty resolver cache

DNS/DNSSEC

Zone:	.	de.	tum.de.
NS:	de.	tum.de.	
DS:	de.	tum.de.	
RRSIG DS:	de.	tum.de.	
RRSIG A:			www.tum.de.
DNSKEY:	.	de.	tum.de.
A:			www.tum.de

17

DNSSEC problems

- Signing and verification are mathematical complex need computational power
- DNSSEC packets are larger than DNS packets
  - Larger memory footprint for servers
  - Higher network bandwidth needs
  - Larger packets ⇒
    - Fragmentation
    - Truncation
    - Fallback from UDP to TCP

  (DNSSEC requires min pkt size: 1220 Bytes (512 DNS)
  recommends pkt size: 4000 Bytes

18

DNSSEC overhead

Type	Overhead (bytes)	Comment
DNSKEY	18 + key size	RSA or ECC
DS	36	SHA-1 digest
RRSIG	46 + key size + |zone| 70 + |zone|	RSA ECC
NSEC	23 + |name| + |label|	

- Typical key sizes in bits:
  - RSA: 1024, 1200 [Kolkman, Gieben, 2004]
  - ECC: 136, 144 [Schroepel, Eastlake, 2004]

19

Results: DNSSEC overhead

Type	Count		DNS size		DNSSEC factor		
					RSA		ECC
	All	Norm	All	Norm	All	Norm	all
Query	32.8M	5.1M	1.5G	0.3G	**1.1**	**1.1**	**1.1**
noErr	20.0M	4.2M	3.7G	0.7	**4.1**	**5.3**	**2.3**
Final	6.8M	2.5M	1.2G	0.5G	6.2	5.7	3.0
Referral	10.9M	1.3M	2.3	0.2G	2.0	2.6	1.6
Empty	2.2M	390K	.2G	44M	**11.7**	**10.6**	**5.2**
NXDomain	1.4M	500K	.2G	57M	**12.7**	**12.9**	**6.2**

- Queries: almost no overhead
- Answers: Final and Referral OK but Empty, NXDomain expensive
- Answers: RSA about twice as expensive as ECC
- Answers: All about the same as normalized

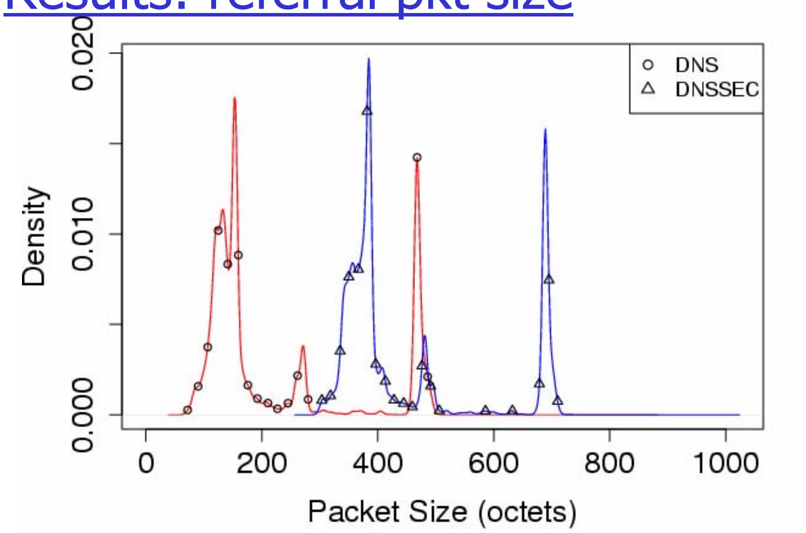
20

Results: packet size

	Size ≤	NXDom	noErr	Final	Ref.	Empty
RSA	1,228	**.005**	.790	**.701**	1	**.633**
RSA	1,480	**.231**	.951	**.921**	1	**.996**
RSA	2.056	.999	.997	.991	1	.999
RSA	4,008	1.000	.999	.999	1	1.000
ECC	1,228	.998	.999	.998	1	.999
ECC	1,480	.999	.999	.999	1	.999

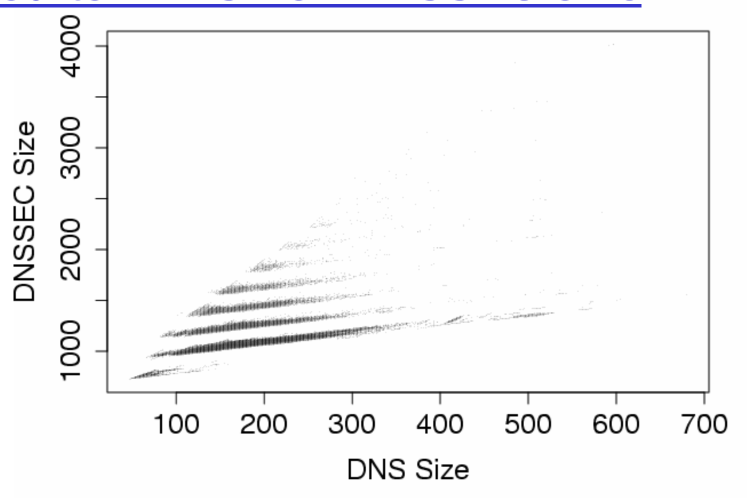
- Dig shows default 2056 bytes, 4008 bytes recommended
- 60% of packets not limited by maximum packet sizes (Query, FormErr, ServFail, Refused packets) but less than 1/3 of DNS size and 1/10th of DNSSEC
- noError, NXDomain problematic NXDomain: 77% (TR02), 72% (TR04) need fragmentation
- ECC: almost no problem...

Results: referral pkt size



- Shapes of densities similar but shifted (+1 DS RR)

Results: DNS vs. DNSSEC size



- Parallel lines: vertical distance 174 bytes
  same number of authorative RRsets

23

CPU usage increase

- Authoritative name servers
  - Due to larger data volume
  - Average CPU usage (five experiments at 1 M queries)

Level	#DNS	CPU-time DNS	#DNSSEC	CPU-time DNSSEC
0	5.0K	1.0s	6.4K	2.03s
1	61.8K	11.56s	65.4K	13.85s
2	176.1K	23.80s	249.1K	39.71s

  - Overhead factor 1.1 to 2
  - Overhead factor per query 1.3 to 1.6

24

CPU usage increase

- Caching name servers
  - Due to verification, larger data, stripping of info
  - 218k queries (averaged over 5 experiments)

cached	CPU-time DNS	CPU-time DNSSEC	Delay DNS	Delay DNSSEC
No	292.8s	665.4s	1.8ms	3.9ms
Yes	37.1s	45.9s	0.2ms	0.2ms

  - Without caching: factor 2.3
  - Absolute additional delay small
  - With caching: factor 1.25

25

Summary

- Examined cost of wide spread DNSSEC deployment
  - Network bandwidth
  - Resource consumption
- Real world analysis from large client population
- Findings:
  - Increase per packets: avg: 3.4 max: 12.7
  - ECC outperforms RSA
  - Higher memory and CPU requirements
- No apparent show stopper!

26