

# DNS Security

Manhee Lee    Ananth Kini

# Agenda

## **DNS Architecture**

**Root vulnerability - DoS**

**Information Leakage**

**Poor Name Server Topology - DoS**

## **DNS Request Reply**

**DNS Cache Poisoning**

**BIND Vulnerabilities**

**Breaking into DNS server**

**DNS configuration lapses**

## **DNSSEC - DNS Security Extension**

**Tree Based Trust**

**Mesh Based Trust**

# DNS Background

# Advent of DNS

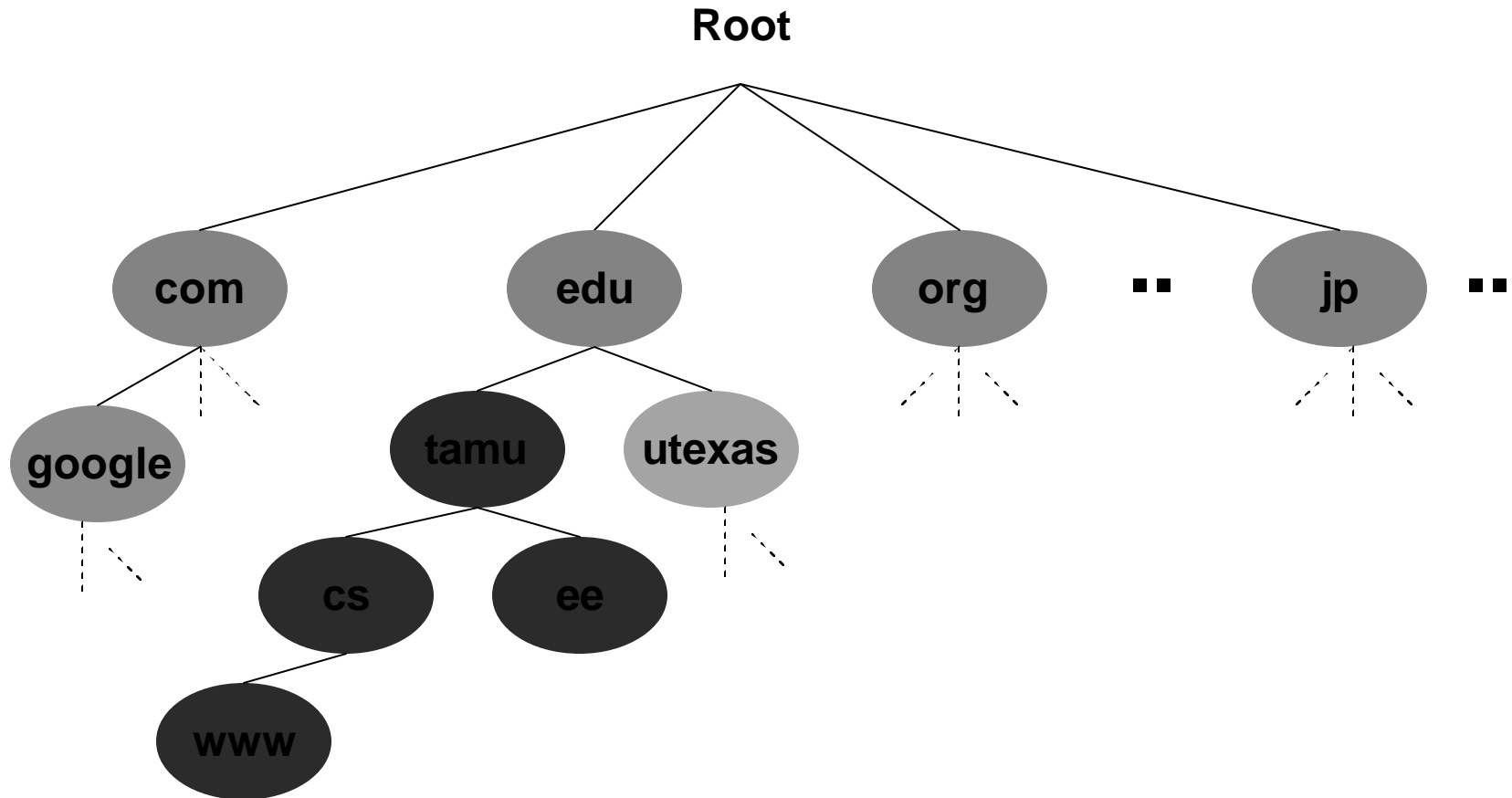
- Humans prefer names to IP addresses  
Prefer foobar to 164.107.51.28
- Simple Solution: Hosts.txt
- Drawback: Not scalable
- Solution: DNS  
(Adopted in 1983)  
RFC 1034, 1035 – '87



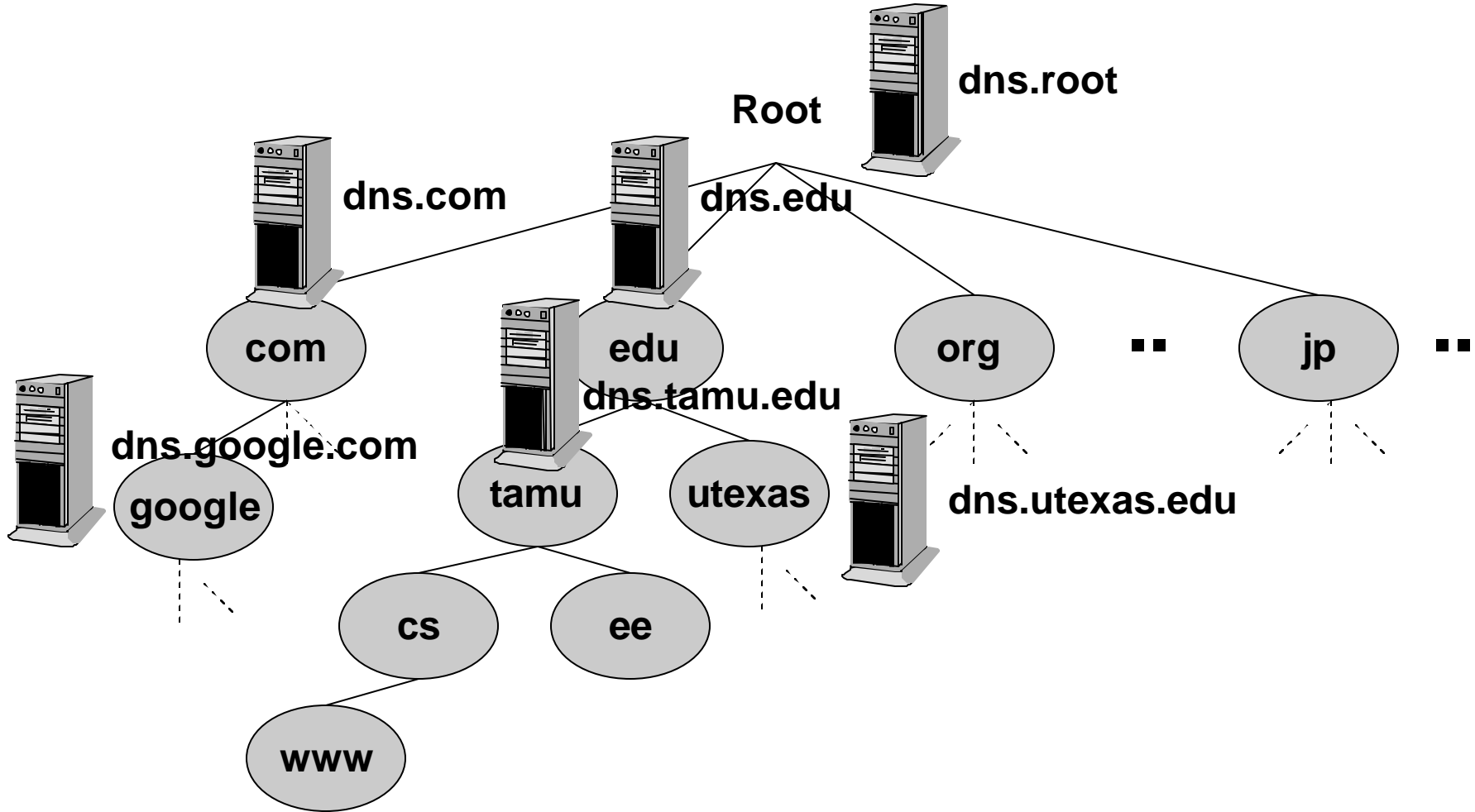
DNS inventor  
Paul Mockapetris

# DNS Architecture

# Name Hierarchy



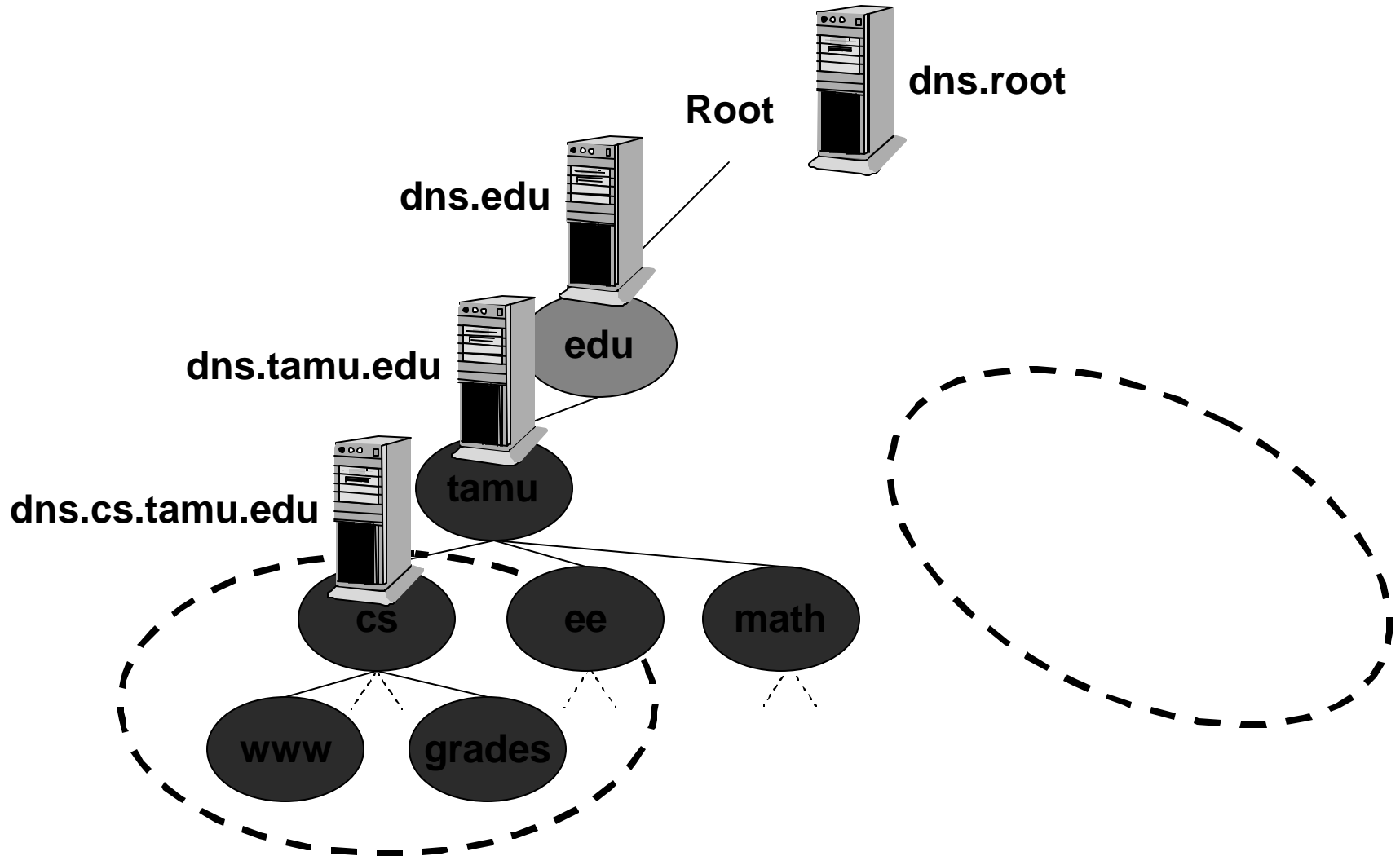
# Server Hierarchy



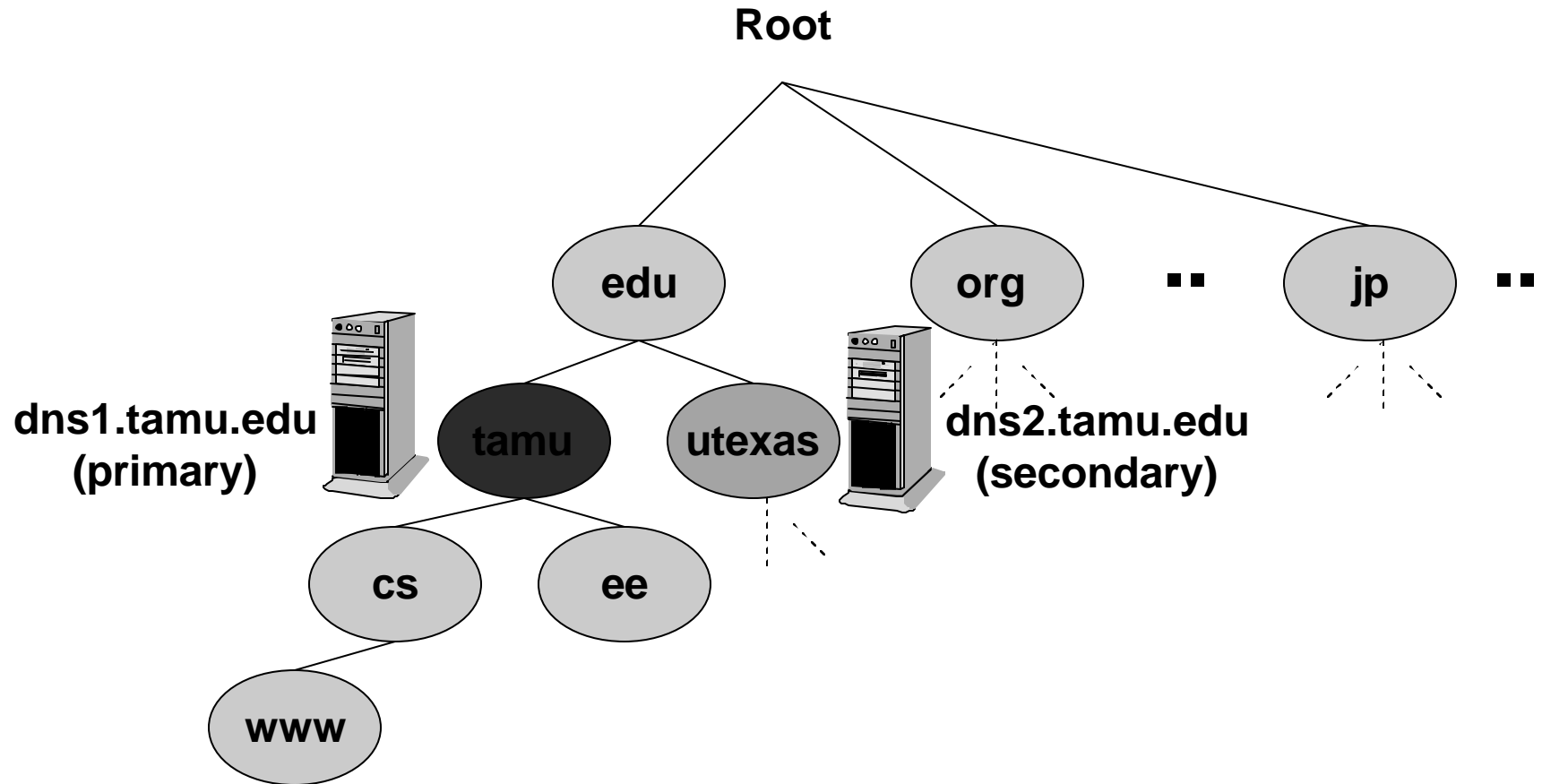
# Root Server

- Root name servers are authoritative for all TLDs
- They know how to get to each TLD name server
- Total of 13 root servers
- Run by different government and commercial organizations throughout the world
- Targets of hacking !

# Zone Delegation



# Primary/Secondary Name Server



Root – A single point of failure

# Attack on Root Server

- OCTOBER 23, 2002
- DDOS on root servers
- 9 out of 13 servers were down
- Slowdown after 8 or more servers are down
- No noticeable slowdown observed by users

# Information Leakage

# Info Leakage - Zone transfer

- Bulk update of secondary name servers
- Provides internal topology information on a platter
- Incremental Zone update
- Spoofed Zone transfer requests
- Access control lists – spoofing still a problem
- Authentication of Zone transfers - TSIG

**RFC 2845 (Shared Secret Key and Message Digest) `00**

# Poor Name Server Topologies

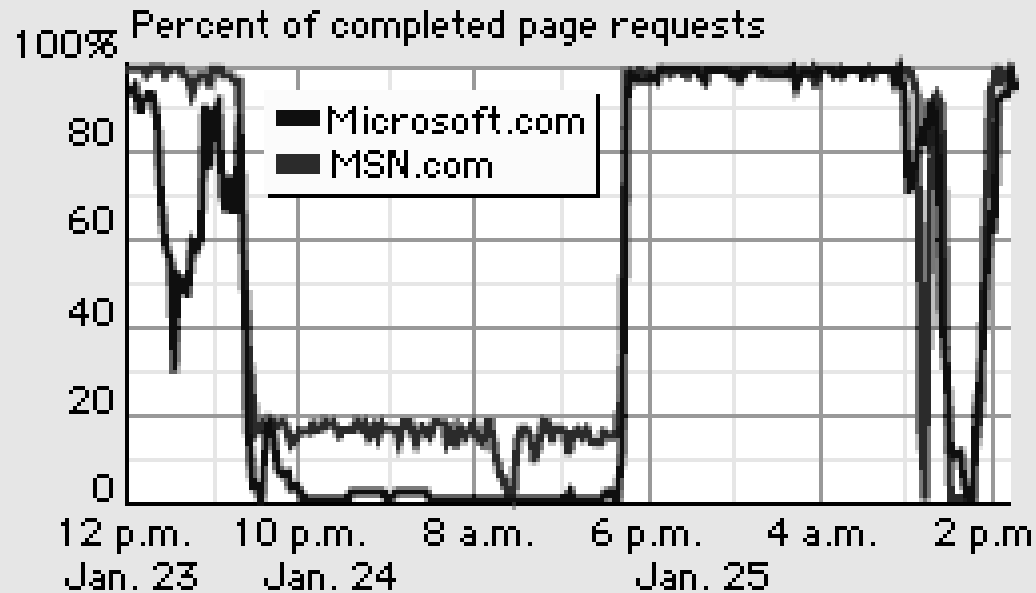
# Attack on Microsoft

- 22.5 hour outage of web sites
- Series of attacks on Name servers, Jan 2001
- Reasons – attack or misconfiguration?
- Intermittent access to Microsoft.com, MSN.com
- \$200 million advertising campaign
- Microsoft Web sites drew 54 million unique visitors in December

# Attack on Microsoft

## Microsoft's mess

Microsoft's Web outage halted service for most of Wednesday and again on Thursday.



Source: Keynote Systems

Normal Days 97%

After attack 2%

# Reasons for Microsoft Attack

- All the DNS servers in a single subnet
- Single router entrance to a series of DNS servers
- Router drowned in a request-response flood
- Legitimate requests suppressed

# Request Reply Architecture

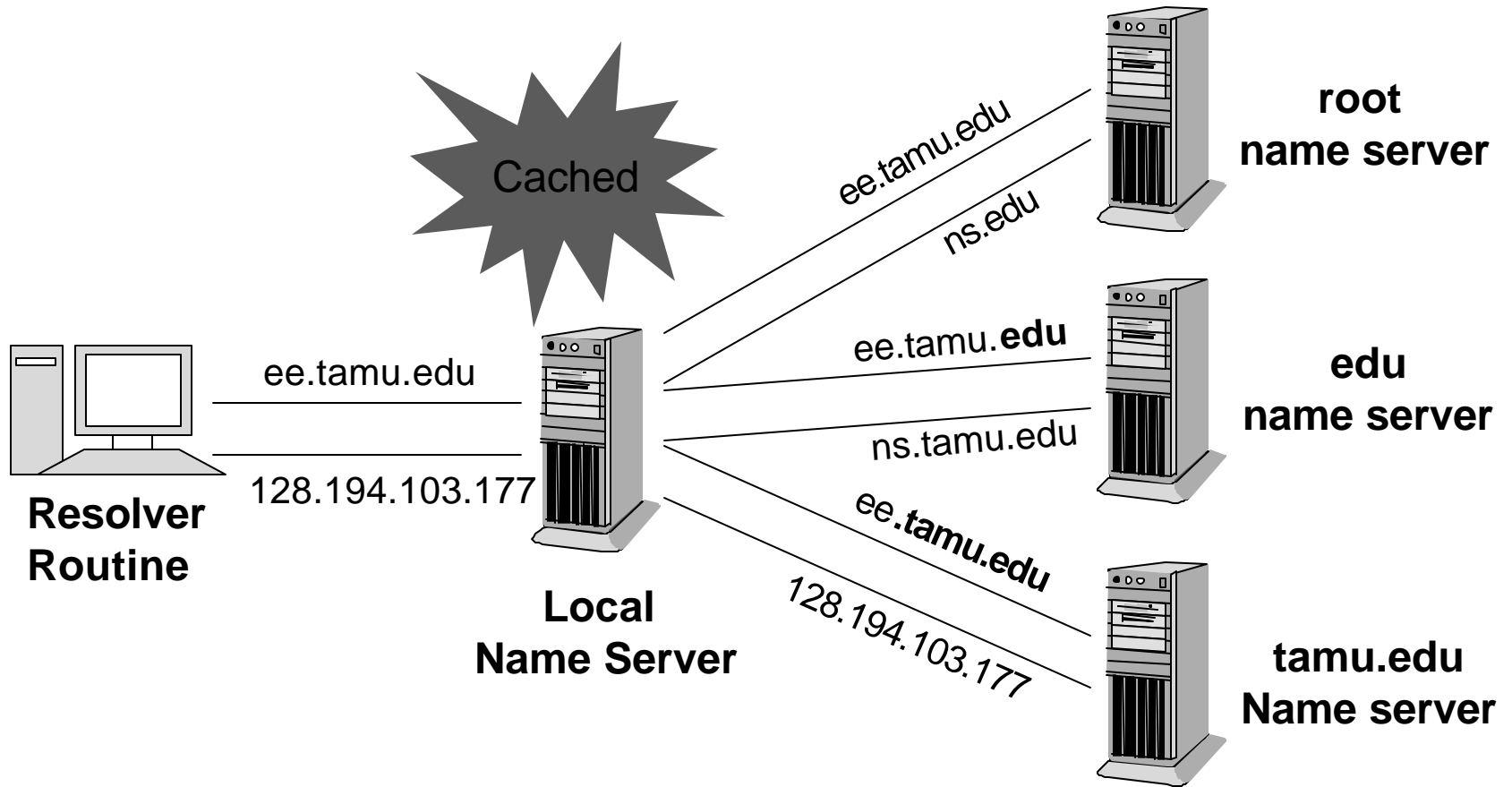
# Resolver

- All hosts must run a DNS resolver routine
- The resolver is linked into each application via a DLL
- It presents an API to user programs. Eg: `gethostbyname` in UNIX
- Given a domain name, it will request a lookup from the Local Name Server

# DNS lookup

- DNS requests are handled either iteratively or recursively
- Iterative - Referral Based
- Recursive - Give me an answer (Don't give me a referral)
- Results may be cached

# DNS lookup - Iterative



# Cache Poisoning

# Cache Poisoning

- Information Poisoning
- Domain Hijacking
- Can occur during Zone transfer
- TTL field of DNS
- Shorter TTL?
- Query nearby “trusted” Name servers?
- Authentication of reply - DNSSEC

# RSA, NIC Domain Hijack

- July 1997 InterNIC website hijacked
- Demonstration against control over DNS by InterNIC
- Feb 2000 RSA website hijacked
- Attack injected bogus entries into cache
- Appeared as though website has been taken over

# Other Security Vulnerabilities...

# Other Security Vulnerabilities...

- BIND Vulnerability

Eg: Transaction ID, Multiple Queries, Buffer Overflow

- DNS Configuration Lapses

Eg: Access control lists

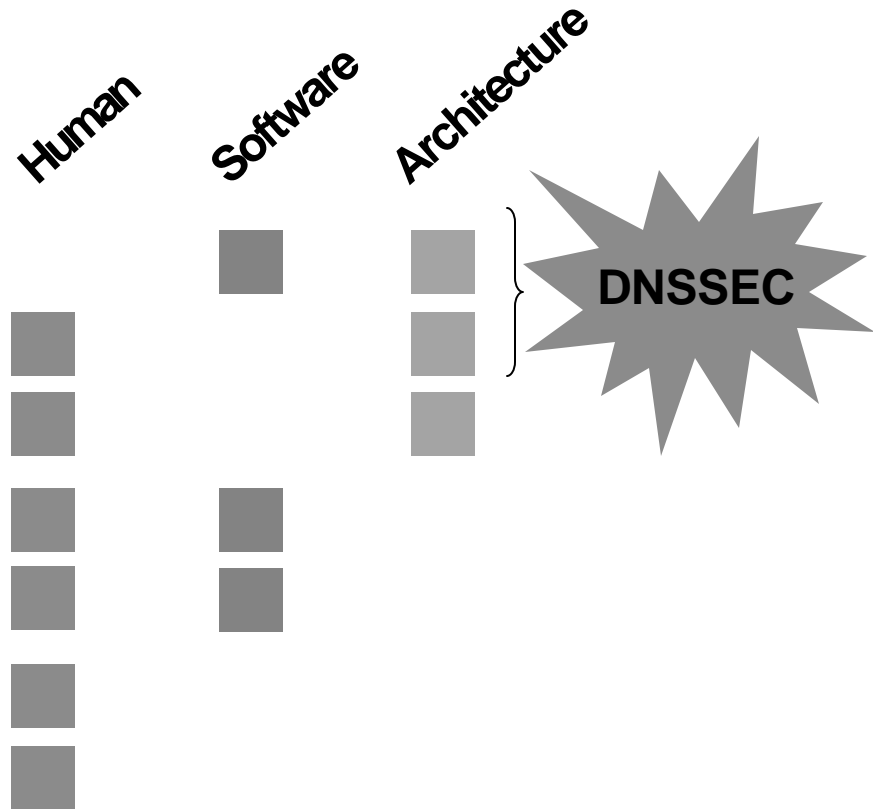
- Breaking into DNS server

Eg: Root process

# Classification of DNS threats

Source of error :

DNS Cache Poisoning
Information Leakage
Denial of Service
Breaking into DNS server
BIND Vulnerabilities
DNS configuration lapses
Poor DNS structure

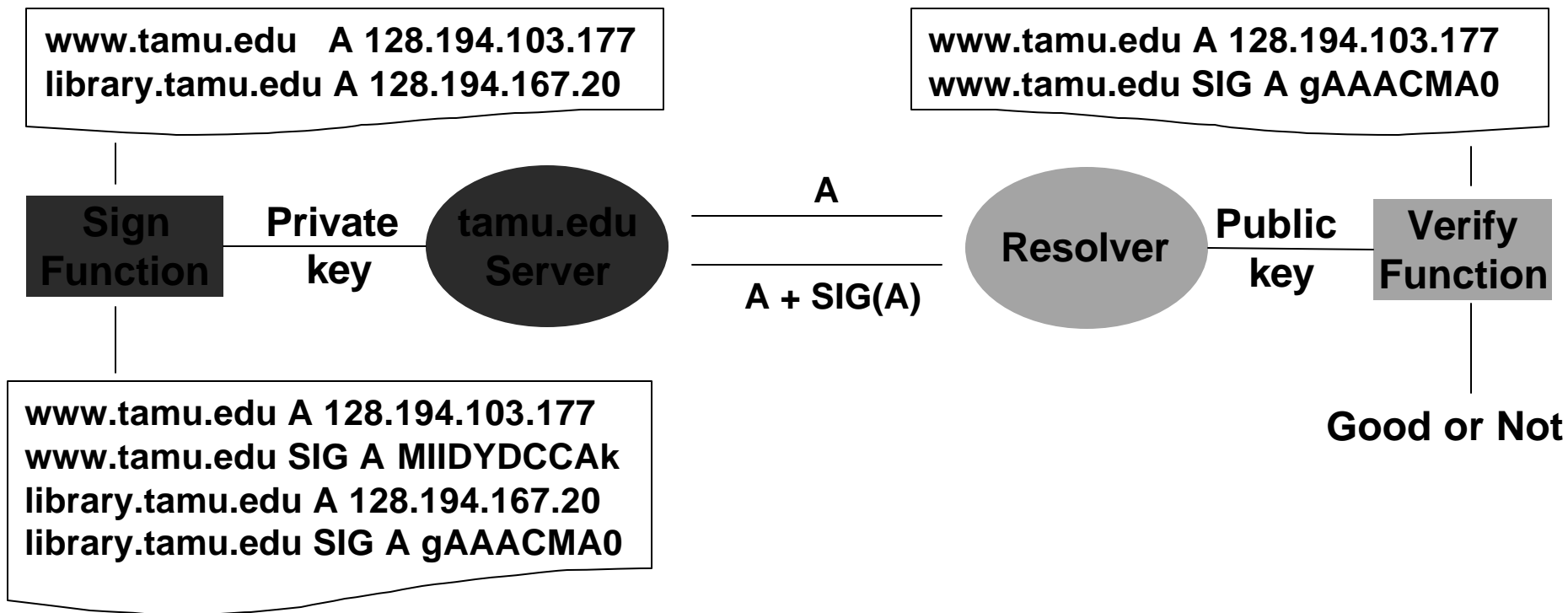


# DNS Security Extension (DNSSEC)

- RFC 2065 -1997, RFC 2535 -1999
- IETF DNS Extensions (DNSEXT) WG
- Idea: Add a digital signature to each Name Information
  - Signing with the zone's private key
  - Authenticating with the zone's public key
- Main issue
  - How to get the public key?
  - DNS as Public Key Infrastructure

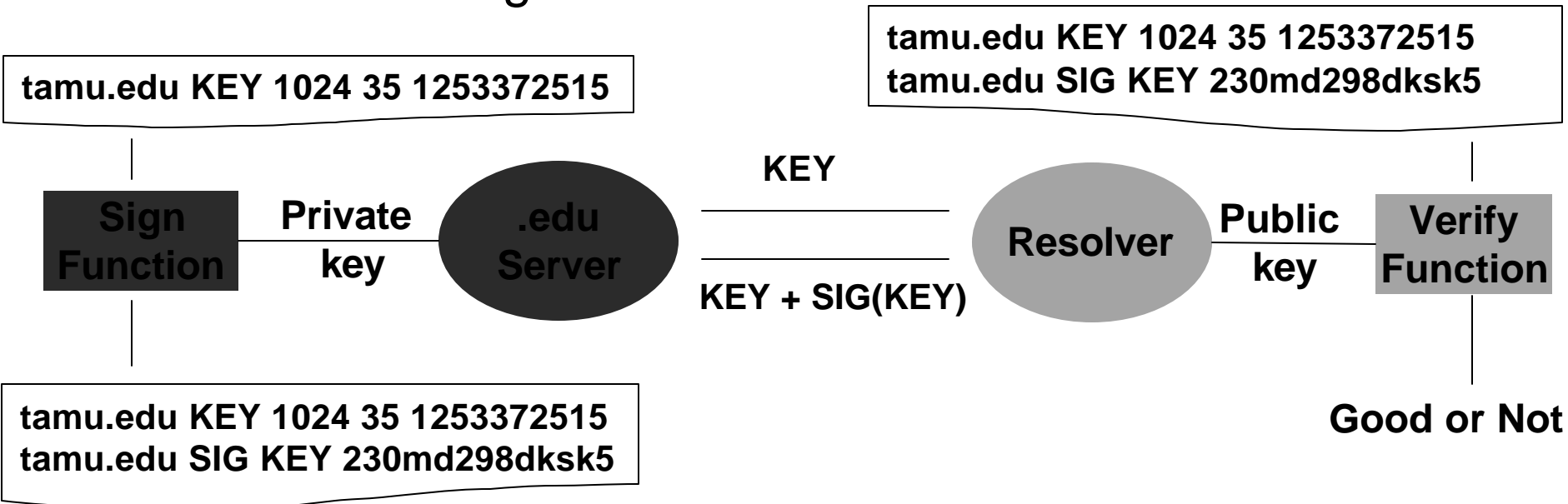
# Name Information Authentication

- SIG Resource Record
  - Signature signed by the zone's private key offline
  - A SIG RR always comes with the signed RR



# KEY Acquisition

- KEY Resource Record
  - Public key of a zone
  - Stored in name server like other RR
  - Need another KEY to sign and authenticate a KEY :  
KEY chaining

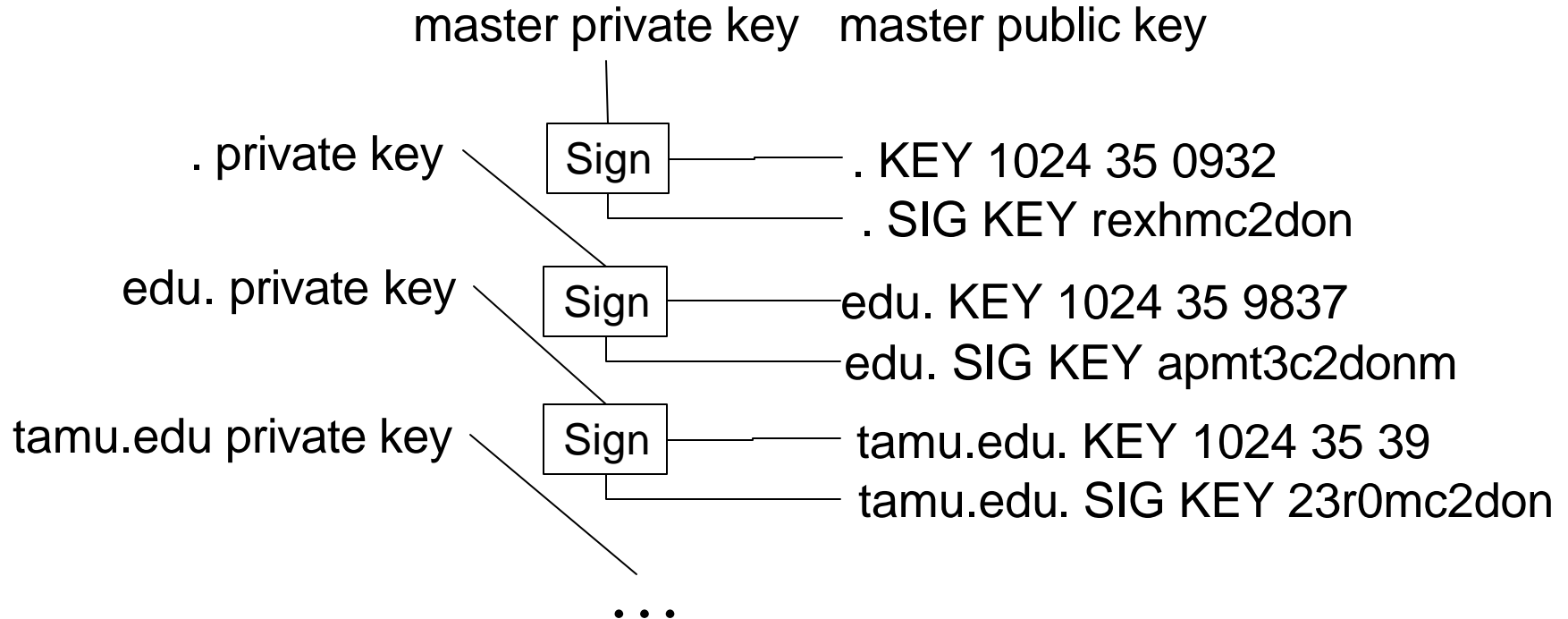


# KEY Chaining

- Who can sign a zone's KEY?
- Tree-based (proposed in RFC2535)
  - ONLY parent zone
  - Easy to find a KEY signer in the parent zone
- Mesh of Trust (proposed by Massey et al.)
  - SOME zones
  - Need additional information about signers

# Tree-based KEY Chaining

- KEY chain: master key → root key → .edu key → tamu.edu key
- Assumption: All resolvers and DNS servers must have the master public key !



# KEY Validation Process

4

root  
■

KEY(.), SIG(KEY)masterkey

3

Q:KEY(.)

KEY(.edu), SIG(KEY)rootkey

2

.edu

Q:KEY(.edu)

A: KEY(tamu.edu), SIG(KEY)edukey

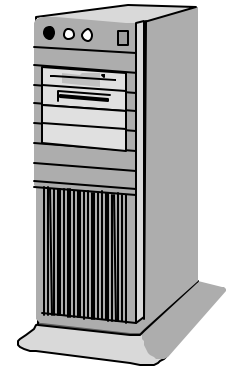
1

tamu.edu

Q:KEY(tamu.edu)

Addr(www.tamu.edu), SIG(Addr)tamukey

Q:A(www.tamu.edu)



Local Name Server

# Pros and Cons of Tree-based

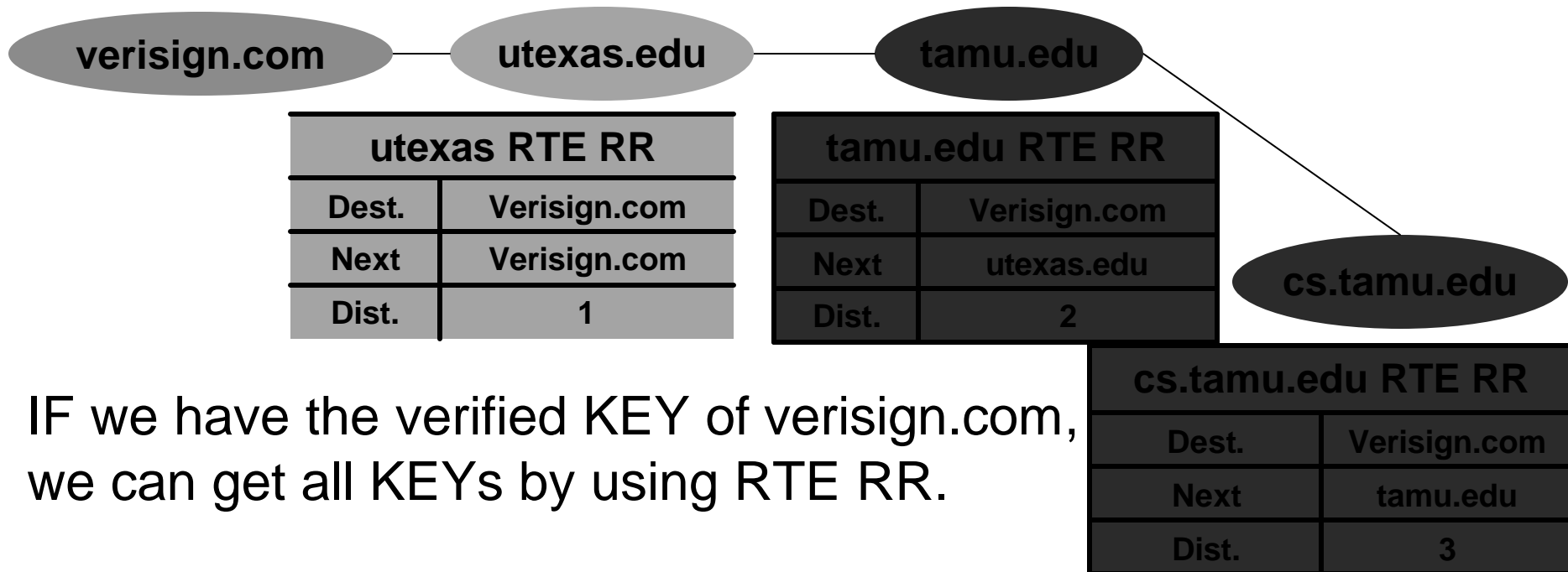
- Pros
  - Universal key signing rule
  - Efficient key chaining
- Cons
  - Incremental deployment
  - Single point of failure
  - Undesirable trust relationship
  - Burden on key signing mechanism

# Mesh of Trust Key Chaining

- Proposed by Massey et al.
- Idea: Not only parent zone, but also other zones can sign
- Ex. verisign.com → utexas.edu → tamu.edu → cs.tamu.edu
- Main issue: Missing KEY chain.
  - RTE RR contains KEY chain information

# Problem transformation

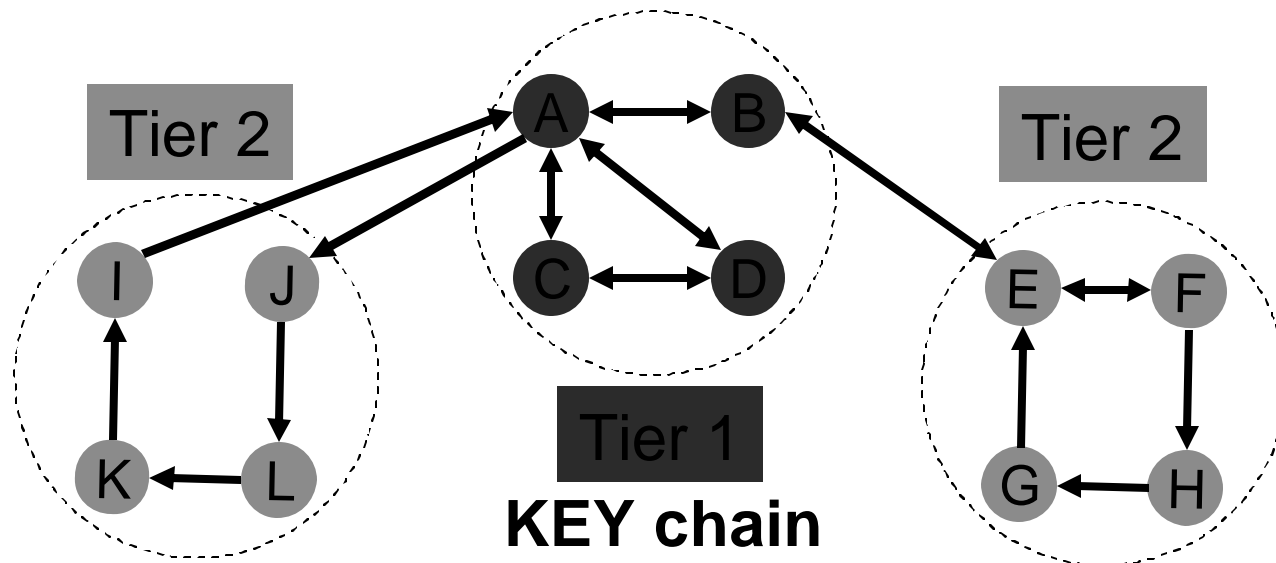
- Key chaining problem -> Finding a path in directed graph
- Ex. verisign.com → utexas.edu → tamu.edu → cs.tamu.edu



IF we have the verified KEY of verisign.com, we can get all KEYs by using RTE RR.

# Two-Tier Mesh Trust

- Tier 1 Mesh: Strongly connected, meaning that each zone has at least one path to every other zone
- Tier 2 Mesh: Each zone has at least one path from and to a zone in Tier 1 Mesh



G->E->B->A->J->L->K

K->I->A->B->E->F->H->G

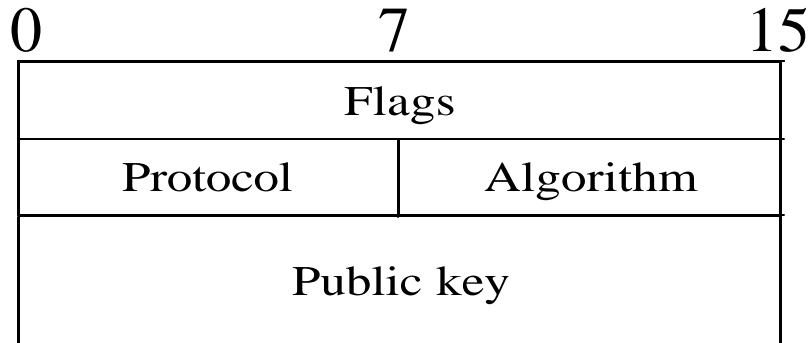
# Advantages of Mesh of Trust

- Ease of deployment
- No single point of failure
- Scalable key signing

# References

- This document
- D.Eastlake, Domain Name system Security Extentions. RFC2535, Internet Engineering Task Force, Mar. 1999.
- [http://www.cse.ohio-state.edu/~jain/bnr/ftp/f24\\_dns.pdf](http://www.cse.ohio-state.edu/~jain/bnr/ftp/f24_dns.pdf)
- [http://www.ists.dartmouth.edu/ISTS/ists\\_docs/intvuln.pdf](http://www.ists.dartmouth.edu/ISTS/ists_docs/intvuln.pdf)
- [http://www.mitretrek.org/publications/sigma\\_pubs\\_winter04/SigmaWinter2004.pdf](http://www.mitretrek.org/publications/sigma_pubs_winter04/SigmaWinter2004.pdf)
- [http://www.giac.org/practical/GSEC/Steven\\_Lau\\_GSEC.pdf](http://www.giac.org/practical/GSEC/Steven_Lau_GSEC.pdf)
- <http://news.com.com/2100-1001-251573.html>
- <http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,86457,00.html>
- [http://www.findarticles.com/cf\\_0/m0FOX/3\\_6/75645162/p1/article.jhtml](http://www.findarticles.com/cf_0/m0FOX/3_6/75645162/p1/article.jhtml)
- [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci519370,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci519370,00.html)
- <http://www.borella.net/mike/MITP432/11%20dns.pdf>

# Appendix: KEY RR



Value	Protocol
0	- reserved
1	TLS
2	Email
3	Dnssec
4	IPSEC
5-254	- available for assignment by IANA
255	All

Value	Protocol
0	- reserved
1	RSA/MD5 (recommended)
2	Diffie-Hellman
3	DSA – MANDATORY
4	Reserved for elliptic curve
5-251	- available
252	Reserved for indirect keys
253	- available
254	Private
255	- reserved

# Appendix: SIG RR

0	15	23	31
Type covered	algorithm	labels	
Original TTL			
Signature expiration			
Signature inception			
Key tag	Signer's name		
signature			

# RRs from CS Name Server

<b>Domain</b>	<b>Type</b>	<b>Class</b>	<b>TTL</b>	<b>Answer</b>
www.cs.tamu.edu.	CNAME	IN	3600	web5.cs.tamu.edu.
web5.cs.tamu.edu.	A	IN	3600	<u>128.194.138.45</u>
cs.tamu.edu.	NS	IN	3600	dns.tamu.edu.
cs.tamu.edu.	NS	IN	3600	dns1.cs.tamu.edu.
cs.tamu.edu.	NS	IN	3600	dns2.cs.tamu.edu.
cs.tamu.edu.	NS	IN	3600	aurora.latech.edu.
dns.tamu.edu.	A	IN	172800	128.194.178.1
dns1.cs.tamu.edu.	A	IN	3600	128.194.138.1
dns2.cs.tamu.edu.	A	IN	3600	128.194.138.2
aurora.latech.edu.	A	IN	86400	138.47.18.3

# RRs from tamu Name Server

<b>Domain</b>	<b>Type</b>	<b>Class</b>	<b>TTL</b>	<b>Answer</b>
www.tamu.edu.	CNAME	IN	600	mimir.tamu.edu.
mimir.tamu.edu.	A	IN	28800	<u>128.194.103.177</u>
tamu.edu.	NS	IN	172800	ns2.tamu.edu.
tamu.edu.	NS	IN	172800	ns3.tamu.edu.
tamu.edu.	NS	IN	172800	aurora.latech.edu.
tamu.edu.	NS	IN	172800	ns1.tamu.edu.
ns1.tamu.edu.	A	IN	172800	128.194.254.4
ns2.tamu.edu.	A	IN	172800	128.194.254.5
ns3.tamu.edu.	A	IN	172800	128.194.254.6
aurora.latech.edu.	A	IN	1398	138.47.18.3