



**FIST Conference**

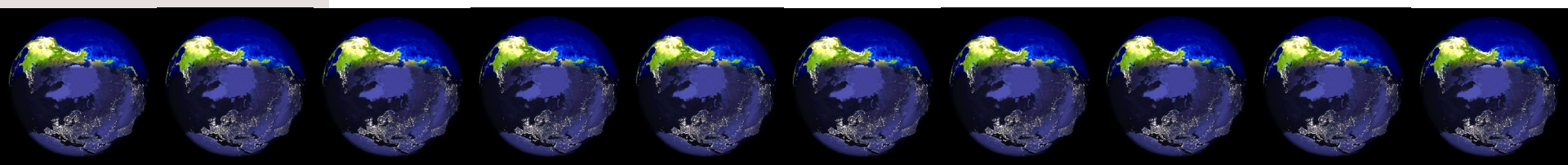
**November 2003 session @ UPSAM**



# **Introduction to DNS Security and DNSSEC**

© Pedro Soria-Rodríguez

[sorrod@alum.wpi.edu](mailto:sorrod@alum.wpi.edu)





# Introduction to DNS

## The Domain Name System

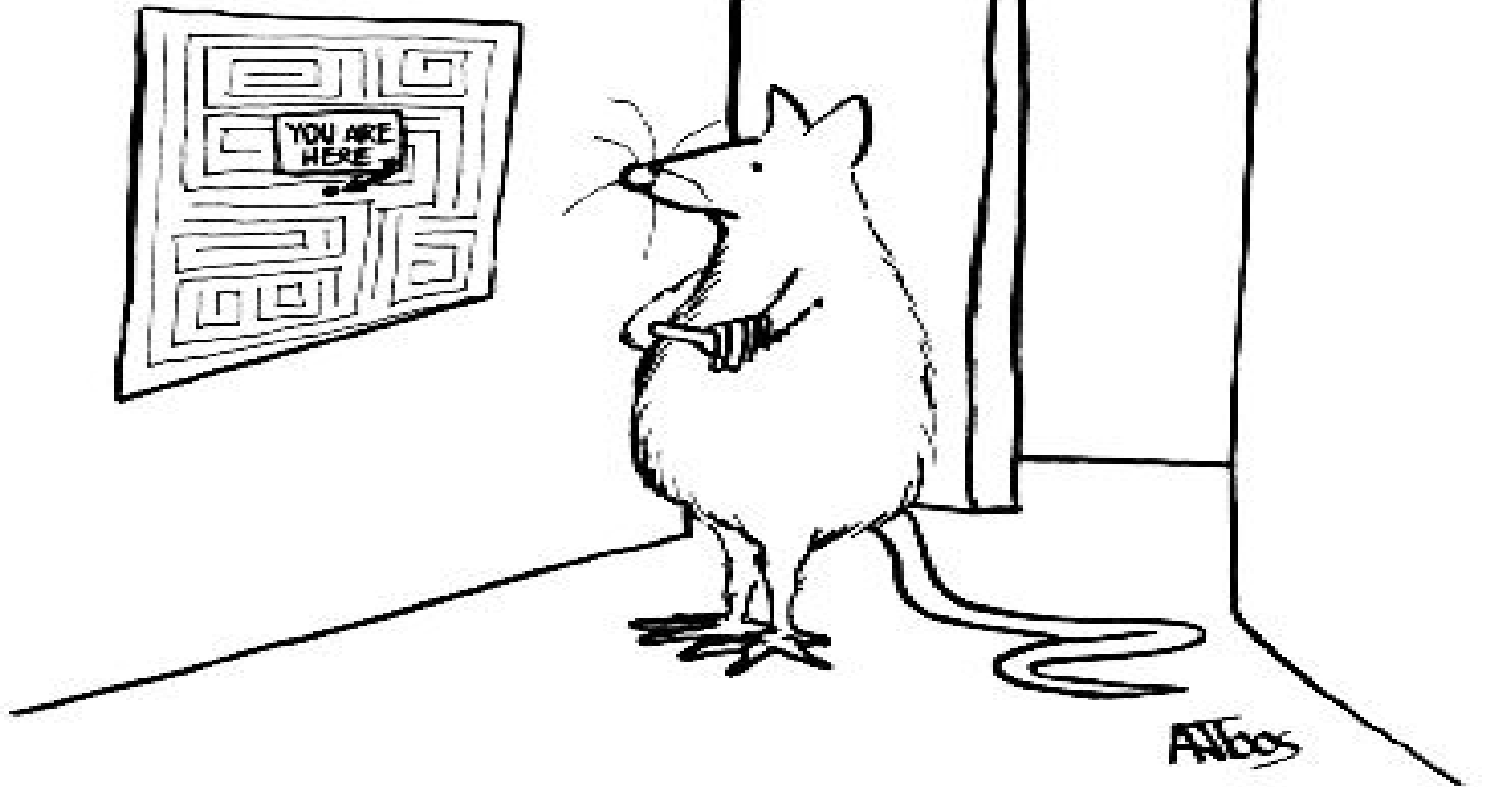
- Idea started in 1982 by Jon Postel
- Created from the need to route email among internet domains

## DNS Services

- Translation of host names to IP addresses
- Routing e-mail to its destination



# Introduction to DNS





# Introduction to DNS

## Parts of the Domain Name System

- DNS Data
- DNS Servers
- Data fetching protocols

## DNS is a . . .

- Distributed
- Replicated
- Hierarchical

. . . database



# Introduction to DNS

## DNS Data

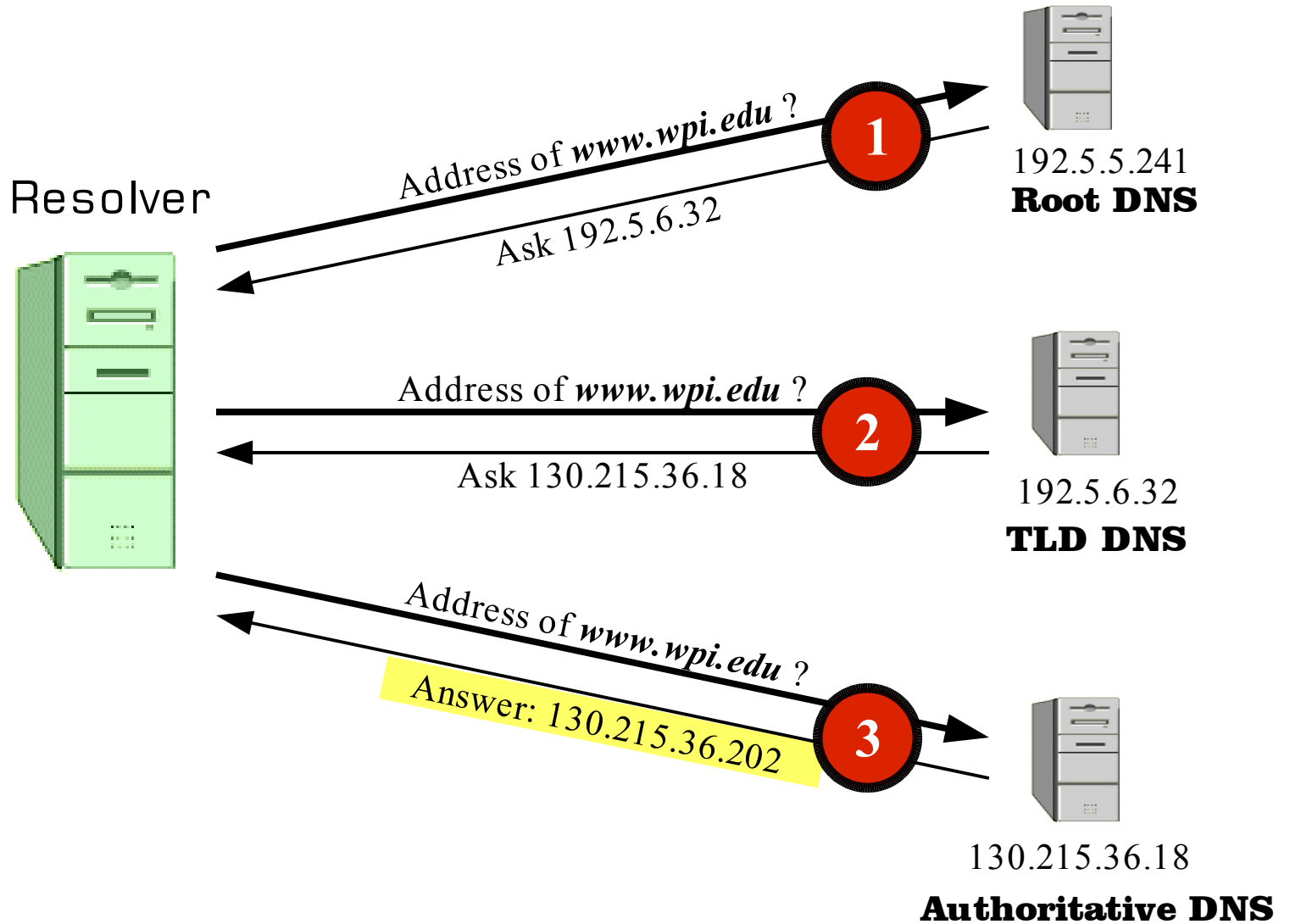
- Types: “Resource Records”
- Organized in “Zone” files

## DNS Servers and Resolvers

- Servers provide information
  - Caching
  - Authoritative
- Resolvers make queries



# Basic DNS operation





# Basic DNS operation

## DNS queries to ask for...

- A hostname's IP address
- A domain's mail exchange
- A hostname's aliases
- Zone transfer (AXFR)

## DNS responses

- “A”, IP address of a hostname
- PTR (pointer), hostname of an IP
- MX (mail exchange), email-processing machine
- Other (AXFR, CNAME, etc...)



# Basic DNS operation

## DNS Zones

- **Zone: All the information regarding a domain**
- **Stored in a primary server**

## Zone transfers

- **For propagating new zone information to secondary DNS servers**
- **Secondary servers poll the primary**



# DNS relevance

**The Internet relies greatly on the DNS**

- **Danger:**
  - **DNS responses lack authentication**
  - **Open to spoofing attacks**



# Problems with DNS

**Several possible attacks:**

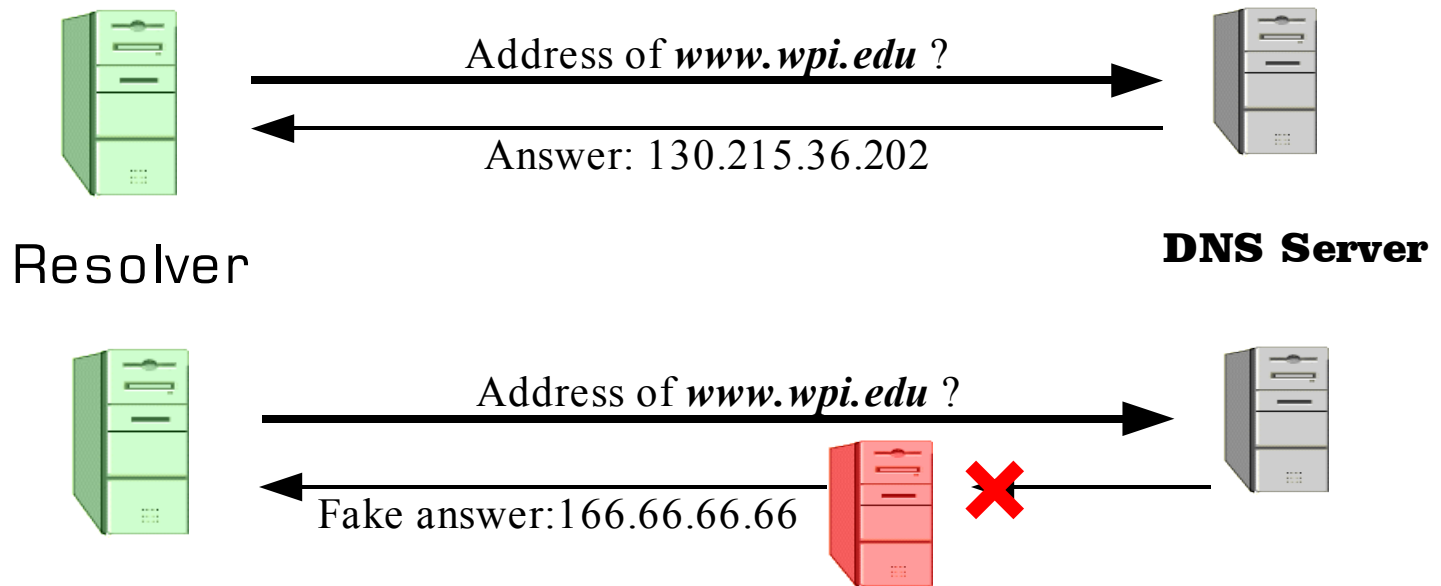
- **Packet interception attacks**
- **Name based attacks**
- **Betrayal by trusted server**



# Problems with DNS

## Packet interception

- DNS responses lack authentication
- DNS responses can be forged



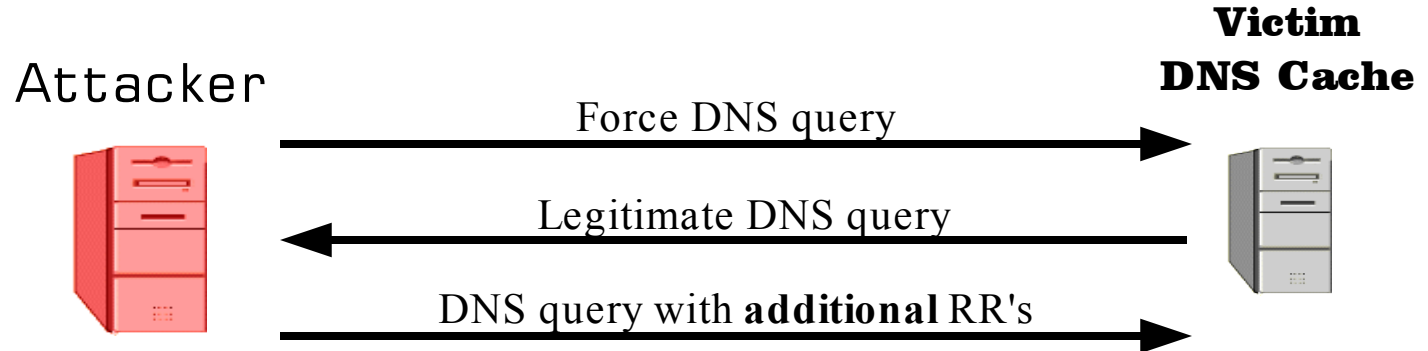


# Problems with DNS

## Name-based attacks

### Cache-poisoning / fake authority

- Injecting RR's with malicious information into a DNS cache

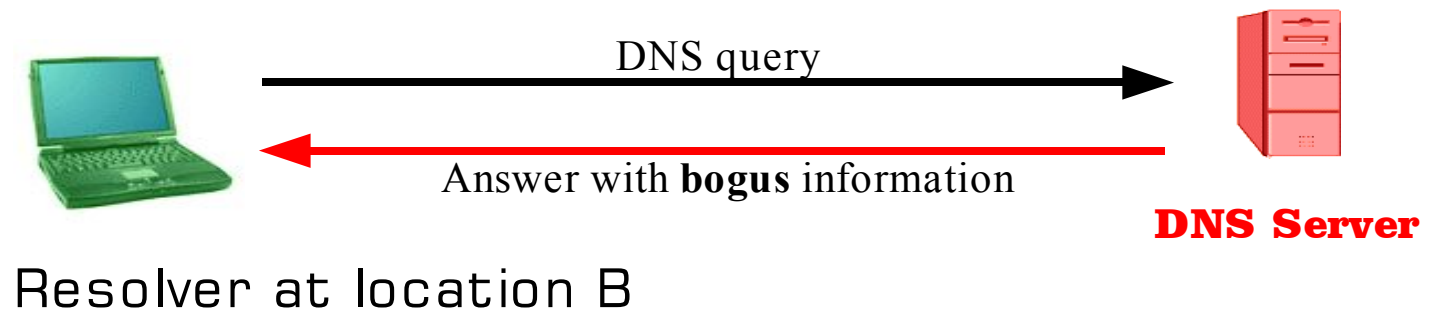
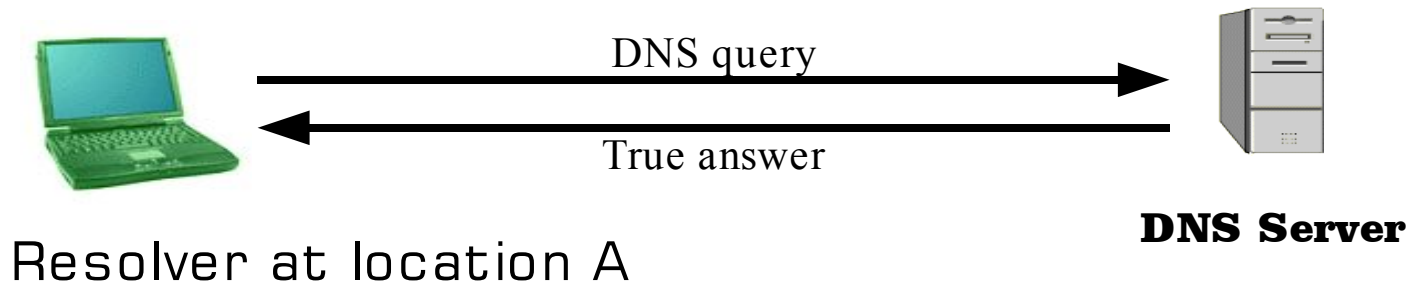


**Additional RR's with DNS names intended to direct new DNS queries to legitimate server belonging to attacker**



# Problems with DNS

Mobile devices trust assigned DNS server





# Solutions for insecure DNS

**Problem is  
lack of authentication**

## **Solution:**

- Introduce authentication and integrity protection
- Using cryptographic signatures



# Solutions for insecure DNS

## TSIG:

- DNS message authentication and integrity
- Request/query authentication
- Transaction authentication

## TKEY

- Establishment of session keys for use in TSIGs

## DNSSEC

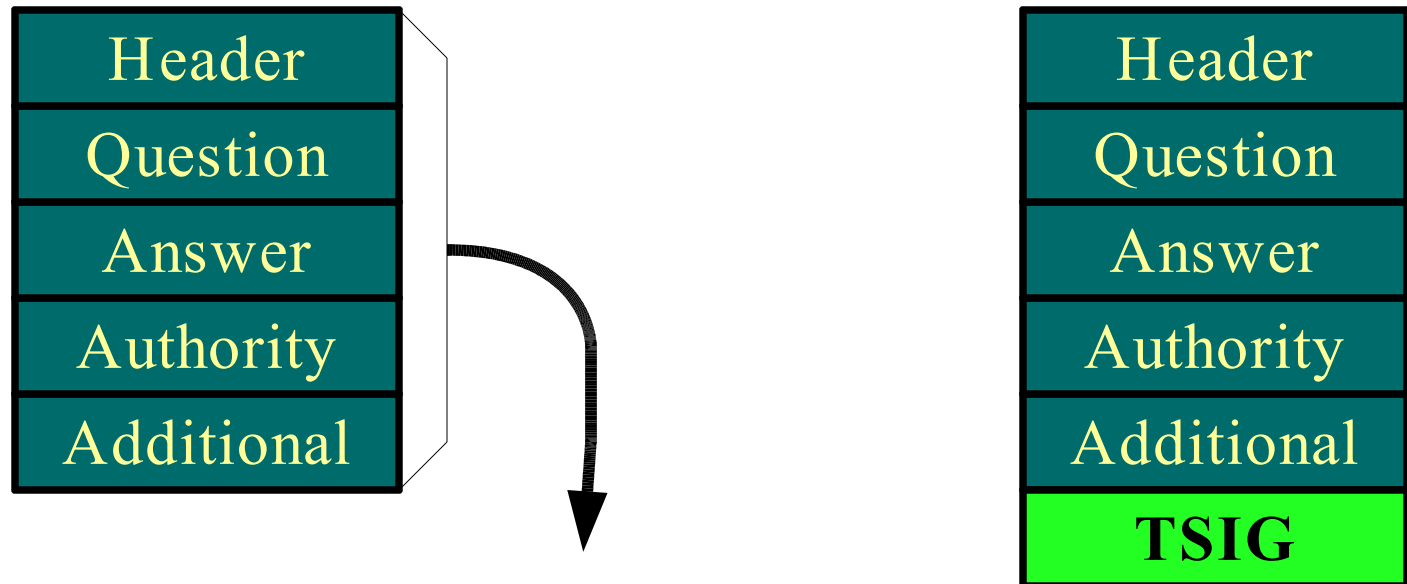
- Zone data protection
- Public key distribution



# Security solutions for DNS

## TSIG – Transaction Signatures

- Symmetric keys
- Signature (keyed hash) appended to messages



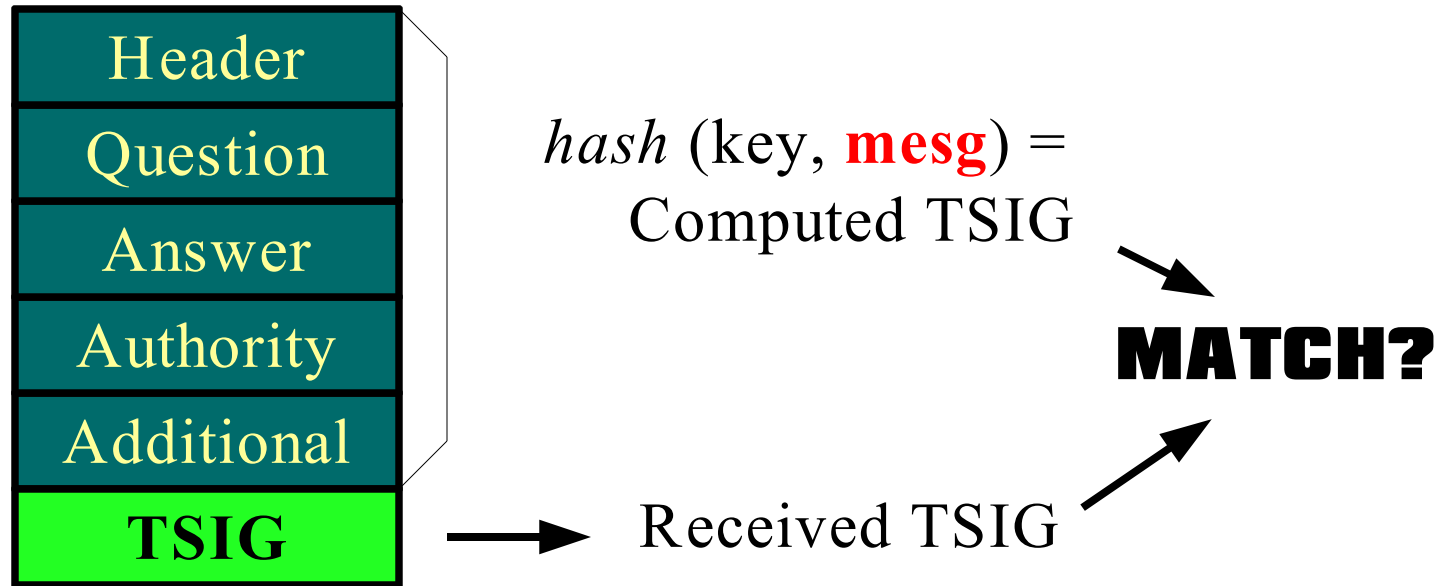
$$\textit{hash}(\text{key}, \text{msg}) = \text{TSIG}$$



# Security solutions for DNS

## TSIG – Transaction Signatures

### Checking the received DNS message







# Security solutions for DNS

## DNSSEC

### Secure Zones

- Every entry in a Zone is signed
- Zones have extra records:
  - SIG – Specify signature of A, MX, SOA, NS records
  - KEY – Specify key of signature
  - SIG – Sign the key
  - NXT – Specify next record in Zone
  - SIG – Signature of the NXT record

### Public Key Infrastructure

- Using DNS as infrastructure to distribute public keys.



# Sample normal DNS Zone file

Examples by Paul Wouters, from <http://www.xtdnet.nl/paul/dnssec/>

```
ct.nl.                IN      SOA      ns.xtdnet.nl. hostmaster.ct.nl. (
                    2003021618 ; Serial
                    28800  ; Refresh
                    7200   ; Retry
                    604800 ; Expire
                    3600)  ; Minimum
ct.nl.                IN      NS       ns.xtdnet.nl.
ct.nl.                IN      NS       ns1.xtdnet.nl.
www.ct.nl.            IN      CNAME    www.fnl.nl.
ct.nl.                IN      MX       10 cable.fnl.nl.
ct.nl.                IN      MX       30 smtp.xtdnet.nl.
```



# Sample secure DNS Zone file

Examples by Paul Wouters, from <http://www.xtdnet.nl/paul/dnssec/>

```
ct.nl.                3600    IN SOA  ns.xtdnet.nl. hostmaster.ct.nl. (
                2003021619 ; Serial
                28800      ; Refresh
                7200       ; Retry
                604800    ; Expire
                3600      ; Minimum
                )
                3600    SIG     SOA 5 2 3600 20030320173018 (
                20030218173018 35861 ct.nl.
                oL3HP9uZnXZMh7SwD3dN )
                3600    NS       ns.xtdnet.nl.
                3600    NS       ns1.xtdnet.nl.
                3600    SIG     NS 5 2 3600 20030320173018 (
                20030218173018 35861 ct.nl.
                9F72hp8M02kUPNOCcPb4 )
                3600    MX       10 cable.fnl.nl.
                3600    MX       30 smtp.xtdnet.nl.
                3600    SIG     MX 5 2 3600 20030320173018 (
                20030218173018 35861 ct.nl.
                S1261RNyGntq+PCZ65xe )
                3600    KEY     256 3 5 (
                XDXiK4oxgbedJx51mDsL
                ) ; key id = 57410
                3600    KEY     256 3 5 (
                8a+qDT/20a1/y2x5slWQ+mgk=
                ) ; key id = 35861
                3600    SIG     KEY 5 2 3600 20030320173018 (
                20030218173018 35861 ct.nl.
                oL3HP9uZnXZMh7SwD3dN )
```



# Security solutions for DNS

## DNSSEC – Does it really exist?

- Still evolving
- Only software that implements it: bind9
- Several proof-of-concept deployments
- Experiment: Dutch NIC and RIPE created first toplevel secure DNS
- Standards (RFCs) being proposed



# Introduction to DNS

## Bibliography

- RFC 1034 “Domain names – Concepts and facilities” (November 1987)
- <http://www.dns.net/dnsrd/docs/whatis.html>
- <http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dns-threats-05.txt>
- <http://www.xtdnet.nl/paul/dnssec/>



**any questions?**

**Introduction to DNSSEC**  
**FIST Conference November 2003**

© Pedro Soria-Rodríguez <[sorrod@alum.wpi.edu](mailto:sorrodp@alum.wpi.edu)>

**Madrid, 28 November 2003**

License: This file may be freely distributed, provided the content is not modified and the notes about authorship are maintained. In all cases, it must be distributed free of charge.