Securing Internet Infrastructure

Ólafur Guðmundsson

ogud@tis.com

Trusted Information Systems

1997 February 10

Talk overview

- Experience in securing
  - DNS
  - Routing protocol
  - DHCP
- My lessons/opinions

Goals of DNSSEC

- Provide design that has minimal impact on the operation of DNS
  - strict hierarchical name space
  - loose consistency distributed database system with caching
    - Pull data distribution model, push is not practical
- Minimize following threats to DNS
  - Incorrect configuration ==> *Wrong or no answer*
  - Data Insertion ==> *Denial of service*
  - Fake nameservers
  - Stale Data ==> *Wrong answer*
  - Incorrect TTL behavior in servers
- Provide cryptographically verifiable bindings between names and records

Securing DNS: DNSSEC

- Adds digital signatures for data source authentication
- Provides public key distribution mechanism
  - ***For free***, Public Keys become regular Resource records
- DNSSEC secures Nameserver to Nameserver but not Nameserver to client (resolver)
  - Data is verified by constructing a chain of KEYS to a trusted key
- Allows servers to explicate deny existence of data.
- Zone is only secure when all parent zones are secure
  - it is harder to attack secured zone than unsecured one.

tis

Key record

```
OWNER NAME, Type: KEY, Class (IN), TTL, RDSIZE,
                        1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             flags             |    protocol   |   algorithm   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               /
   /                          public key                           /
   /                                                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
```

```
For RSA Algorithm, public key
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | pub exp length|        public key exponent                    /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               /
   +-                          modulus                             /
   |                                                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-/
```

Signature Record

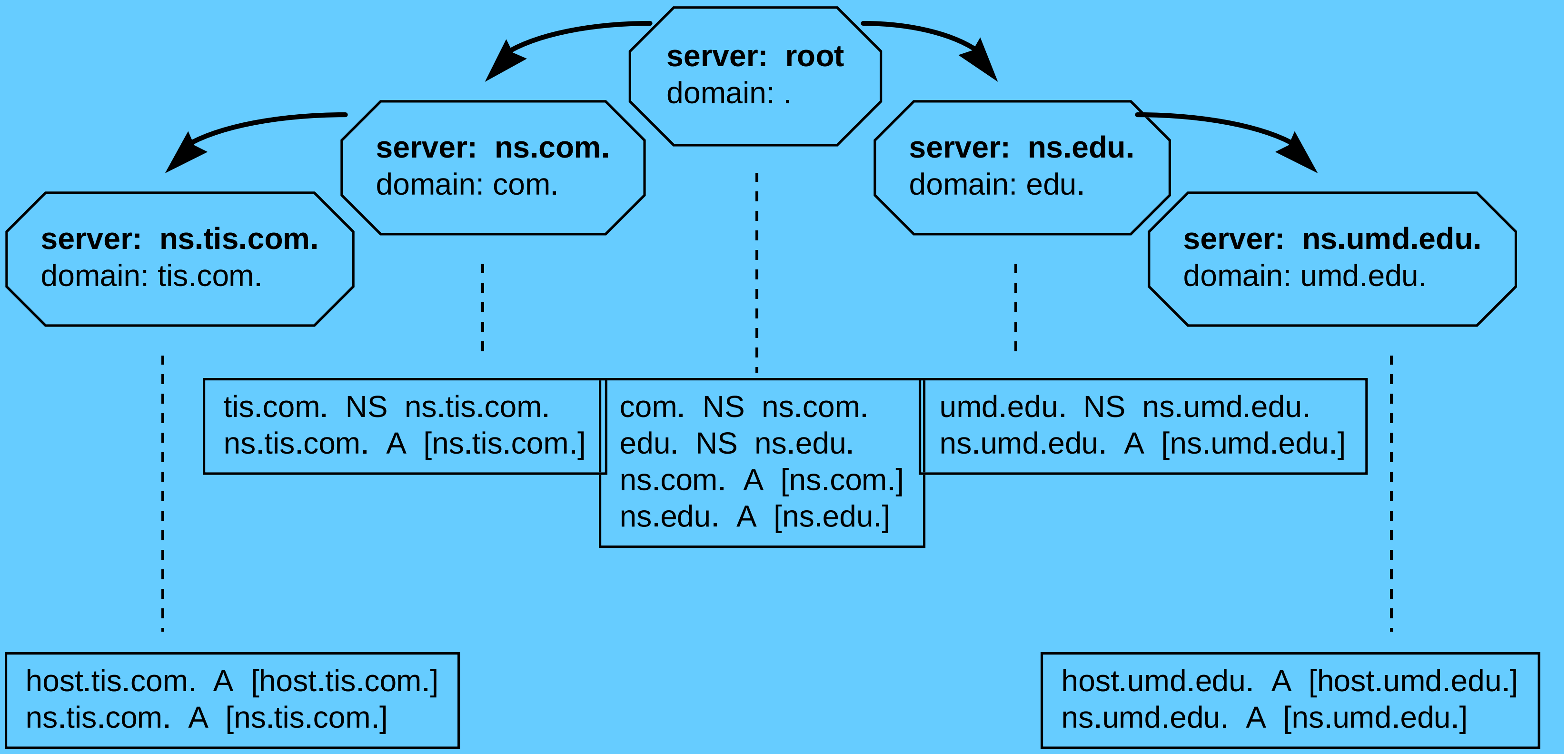
```
OWNER NAME, Type: SIG, Class (IN), TTL, RDSIZE,
                        1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        type covered           |  algorithm    |     labels    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         original TTL                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      signature expiration                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         time signed                           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         key footprint         |                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+        signer's name          /
   /                                                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               /
   +                          signature                            /
   /                                                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Non existence Denial

- Current DNS lacks authoritative non-existence
  - for non-existent domain name you get an “empty” response with name error bit set in the headers;
  - for non-existent resource record client may ask for “ANY” records but must assume server has returned them all
- New resource record type: NXT
  - for each existing name indicate following existing name in zone; zone name space is treated as a ring
  - bit map to indicate presence of types

tis

Domain Name System: Example



server: root
domain: .

server: ns.com.
domain: com.

server: ns.edu.
domain: edu.

server: ns.tis.com.
domain: tis.com.

server: ns.umd.edu.
domain: umd.edu.

tis.com. NS ns.tis.com.
ns.tis.com. A [ns.tis.com.]

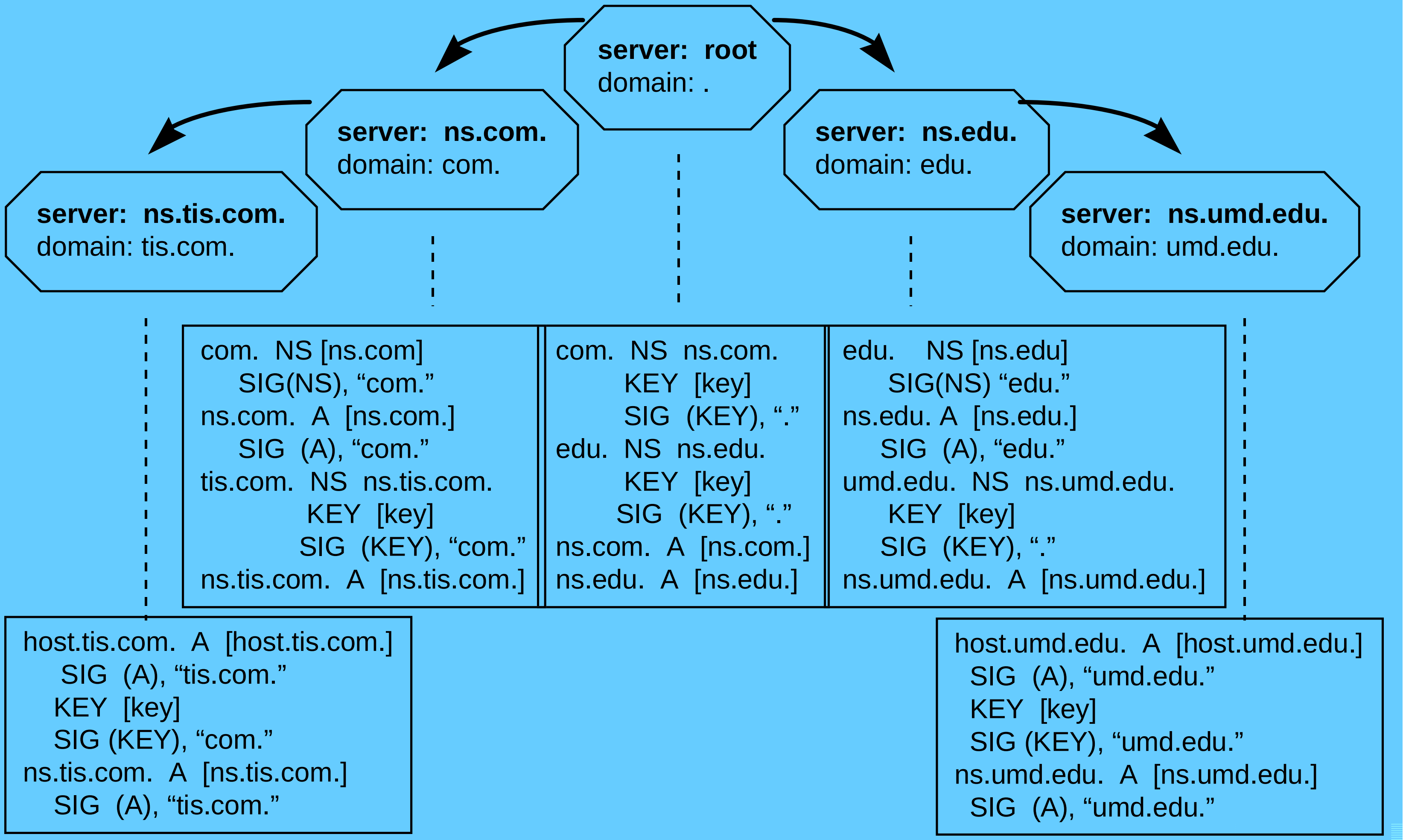
com. NS ns.com.
edu. NS ns.edu.
ns.com. A [ns.com.]
ns.edu. A [ns.edu.]

umd.edu. NS ns.umd.edu.
ns.umd.edu. A [ns.umd.edu.]

host.tis.com. A [host.tis.com.]
ns.tis.com. A [ns.tis.com.]

host.umd.edu. A [host.umd.edu.]
ns.umd.edu. A [ns.umd.edu.]

DNSSEC



server: root
domain: .

server: ns.com.
domain: com.

server: ns.edu.
domain: edu.

server: ns.tis.com.
domain: tis.com.

server: ns.umd.edu.
domain: umd.edu.

```
com.  NS [ns.com]
    SIG(NS), "com."
ns.com.  A  [ns.com.]
    SIG  (A), "com."
tis.com.  NS  ns.tis.com.
           KEY  [key]
           SIG  (KEY), "com."
ns.tis.com.  A  [ns.tis.com.]
```

```
com.  NS  ns.com.
       KEY  [key]
       SIG  (KEY), "."
edu.  NS  ns.edu.
       KEY  [key]
      SIG  (KEY), "."
ns.com.  A  [ns.com.]
ns.edu.  A  [ns.edu.]
```

```
edu.    NS [ns.edu]
     SIG(NS) "edu."
ns.edu. A  [ns.edu.]
    SIG  (A), "edu."
umd.edu.  NS  ns.umd.edu.
     KEY  [key]
    SIG  (KEY), "."
ns.umd.edu.  A  [ns.umd.edu.]
```

```
host.tis.com.  A  [host.tis.com.]
    SIG  (A), "tis.com."
   KEY  [key]
   SIG (KEY), "com."
ns.tis.com.  A  [ns.tis.com.]
   SIG  (A), "tis.com."
```

```
host.umd.edu.  A  [host.umd.edu.]
  SIG  (A), "umd.edu."
  KEY  [key]
  SIG (KEY), "umd.edu."
ns.umd.edu.  A  [ns.umd.edu.]
  SIG  (A), "umd.edu."
```

DNSSEC status

- Proposed Standard RFC 2065
- Exportable reference implementation available
  - www.tis.com./docs/dns.html
  - RSAREF/RSAEURO not included
- We are in the process of merging the DNSSEC changes into Bind production release
- Secure zone available to test against
  - sd-bogus.tis.com. Server: uranus.hq.tis.com.
- We have signed the largest zone COM.
  - contains 754789 names
  - took 38 hours on 166Mz Pentium

tis

DNSSEC future

- Operational issues
  - Need large enough number of high level domains to convert to DNSSEC before we start seeing advantages
  - Certification of keys for zones that have insecure parents.
  - Out of Band protocol transmitting keys to and from signing authorities (Moss, PGP ??)
- Resolver (last hop) issues
  - Servers do not have time for generating RSA signatures
  - Clients are stateless and do not have time to collect all the keys to construct valid key chain.
  - there is a need for inexpensive transaction signature between server and resolver.
    - TSIG proposal suggests how to do this.
  - Need new standard resolver routines that understand security

DNS Dynamic Update

- Authentication of Dynamic Update request
  - Client signs the RR set’s before sending to server, when authorized
  - Client appends a transaction signature to Update request
    - TSIG
- Updates of Server signed data
  - Server needs a private key on line
  - Server must update SOA record
  - Server may need to update NXT records and/or NXT chain
  - Primary server must push data to secondary servers
    - DNS Notify option is designed for this
- Internet draft in RFC queue

Routing

- To provide robust routing operation in the Internet in the face of accidental or malicious failure from
  - external source:
  - internal source: one misconfigured, faulty, or subverted router

Routing

- Routing Algorithm Categories
  - link state
    - determine state of link to each neighbor
    - send link information to every node in the network (using flooding technique)
  - distance vector
    - determine best route to every node in the network (based on route information received from neighbor)
    - send route information to each neighbor
- Difference Between Categories
  - send information about each neighbor to the whole network

  vs.

  - send information about whole network to each neighbor

Securing OSPF

- Protection from external vulnerabilities
  - Simple password authentication
  - MD5 authentication based on a shared secret
- Protection from internal vulnerabilities
  - digital signature of routing information for source authentication (as suggested by Perlman, IDPR, etc..)
  - protection of age field when maximum value is used
- Remaining vulnerabilities
  - OSPF aggregation points (area border routers and external routers) must be believed
  - routers must be trusted to speak about their own links

tis

Securing BGP/IDRP

- Protection from external vulnerabilities
  - Shared Secret authentication
- Protection from internal vulnerabilities
  - digital signature of AS-path “distance” could be included in distance vector
  - could coordinate with route/policy registries to verify authenticity of advertised AS-paths
    - Political problem: ISPs do not want to share information about policies

Securing DHCP

- Dynamic Host Configuration Protocol currently is used to configure computers as they are attached to networks.
- There is no security in current protocol.
- Proposed mechanism include a password based schema and a Shared Secret Authentication of packets
- Shared secret authentication
  - works well if client connects to few servers.
  - Digital signatures needed for clients that connect to large umber of servers

tis

DHCP Problems

- Protocol is used to give computer addresses and identies on a *“random”* network.
- The computer has only MAC address and in many cases limited computing power and storage.
- Legacy systems

Fundamental Problems

- Many Infastructure protocols can not depend on availability of other protocols
  - Routing can not assume it can look up keys with DNS as there is no routing available
- All or nothing
  - Security solutions are not “Effective” until all cooperating systems are secured
- Legacy systems
  - This is becoming less of an issue than it used to be thanks to cheaper hardware, and demands for new “Features”.

Where are we ?

- We are at an important juncture
- Community sees need for additional security functions
  - and is willing to accept the cost of security
- Solutions are being proposed
- We need to get the solutions
  - standardized
  - deployed in products
  - accepted and used

How can we go from here to there

- Deploying solutions that solve most of problem, is *preferable* than waiting for perfect solution
  - We can not protect against everything
  - We need to strike the right balance between
    - needs and requirements
    - false sense of security
  - New protocols need to be designed to accommodate security better than today’s protocols
- Security Challenges change over time
- **Educate user communities**

tis

End of Presentation

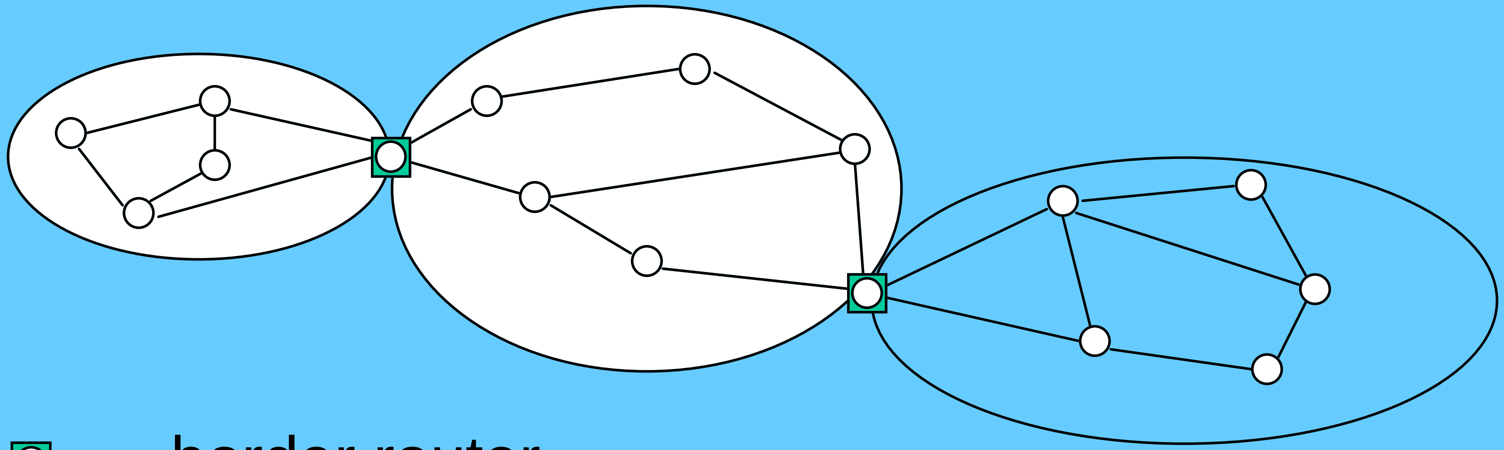
- ogud@tis.com

Securing Multicast

- Multicast Security significant issues
  - routing
    - self-organization of distribution in real-time into one or more directed graphs
    - authentication of paths between nodes,
  - management of multicast functions
    - group membership authorization and restrictions
    - authentication of group member activities
  - Data integrity
    - Authentication for some
    - Confidentiality for others
  - key management

Routing definitions

- Protocol categories
  - inter-autonomous systems
  - intra-autonomous systems



▣ border router

⬭ autonomous system

Types of Routing Protocols

PROTOCOLS IN USE IN THE INTERNET

	inter-autonomous system	intra-autonomous system
link state	IDPR	OSPF IS-IS
distance vector	BGP IDRP	RIP

(not a complete list)