nominet

How Crucial is DNS security in securing the Internet

Roy Arends

Nominet Research Fellow

What is the Domain Name System?

- **DNS is the 'Phonebook' of the Internet**

- All connected devices essentially use the DNS in some form
- The DNS is used to lookup the address for a domain name.
- www.cto.int is a domain name, a DNS lookup will return its address: 70.33.246.199
- DNS provides much more than just addresses.

Original DNS requirements, 1983

- DNS Design Requirements:
  - Fault Tolerant
  - Dynamic
  - Scalable
  - Redundant where needed
  - See RFC799 and RFC819

- The solution added a very important feature:
  - Delegation of authority
  - RFC 1034/1035
- Security was not considered

DNS, how it works

nominet

- DNS is both a network and a namespace.
- Consists of servers that publish a section of the name space, and resolvers that query the servers about the name space
- Attributes are stored in records and individually retrievable
  - Attributes can be anything, but are mostly addresses
- No single system contains all the DNS data

High level concept of DNS

nominet

- Your laptop has a DNS resolver configured
  - The DNS resolver typically resides at an ISP.
- A resolver knows where the root-zone is
- Each level refers the resolver to the next level
- Traverses the DNS hierarchy
  - Root to INT
  - INT to CTO.INT
  - CTO.INT to WWW.CTO.INT
- Until the question has been answered
- The resolver caches all that information for future use.

More detailed

- Domains such as www.bbc.co.uk form a path
  - from the root, through “uk” and other labels, to “www”

- Every level has a set of servers that points (delegates) to the servers of the next level

- The last level of servers contain the address for the domain name.

More detailed

- This hierarchy is traversed by a resolver
  - Typically at an ISP
- It knows the addresses of the root servers
- Asks the root for the answer, and gets referred to the next level.
- Caches whatever it sees for a period of time

No Security

- DNS uses mostly UDP, not TCP
  - UDP is much faster than TCP
- Thus there is no handshake
  - Thats why UDP is much faster than TCP
- There is no guarantee the answer came from the right source
- Or that it hasn't been tampered with in transit
  - This is called "spoofing"
- Caching amplifies the problem
  - This is called "Cache-Poisoning"

DNSSEC is the solution

nominet

- DNSSEC uses **digital signatures** to assure that information is correct and came from the right place.
- The keys and signatures to verify the information, is stored in the DNS as well
- Since DNS is a lookup system, keys can simply be looked up, like any data.

High level concept of DNSSEC

nominet

- A resolver knows what the root-key is

- It builds a Chain of Trust:
  - Each level signs the key of the next level
  - Until the chain is complete

DNSSEC

nominet

- DNSSEC is crucial to online safety
- DNSSEC Tools, servers and services are available today
- Automation of every process is under way.
- Eventually, DNSSEC will be mainstream
  - Just like HTTPS for web-traffic
  - Just like SSH for Telnet traffic

DNSSEC

- With DNSSEC, the DNS is:
  - Fault Tolerant
  - Dynamic
  - Scalable
  - Redundant where needed
  - Distribution of authority
  - Very secure

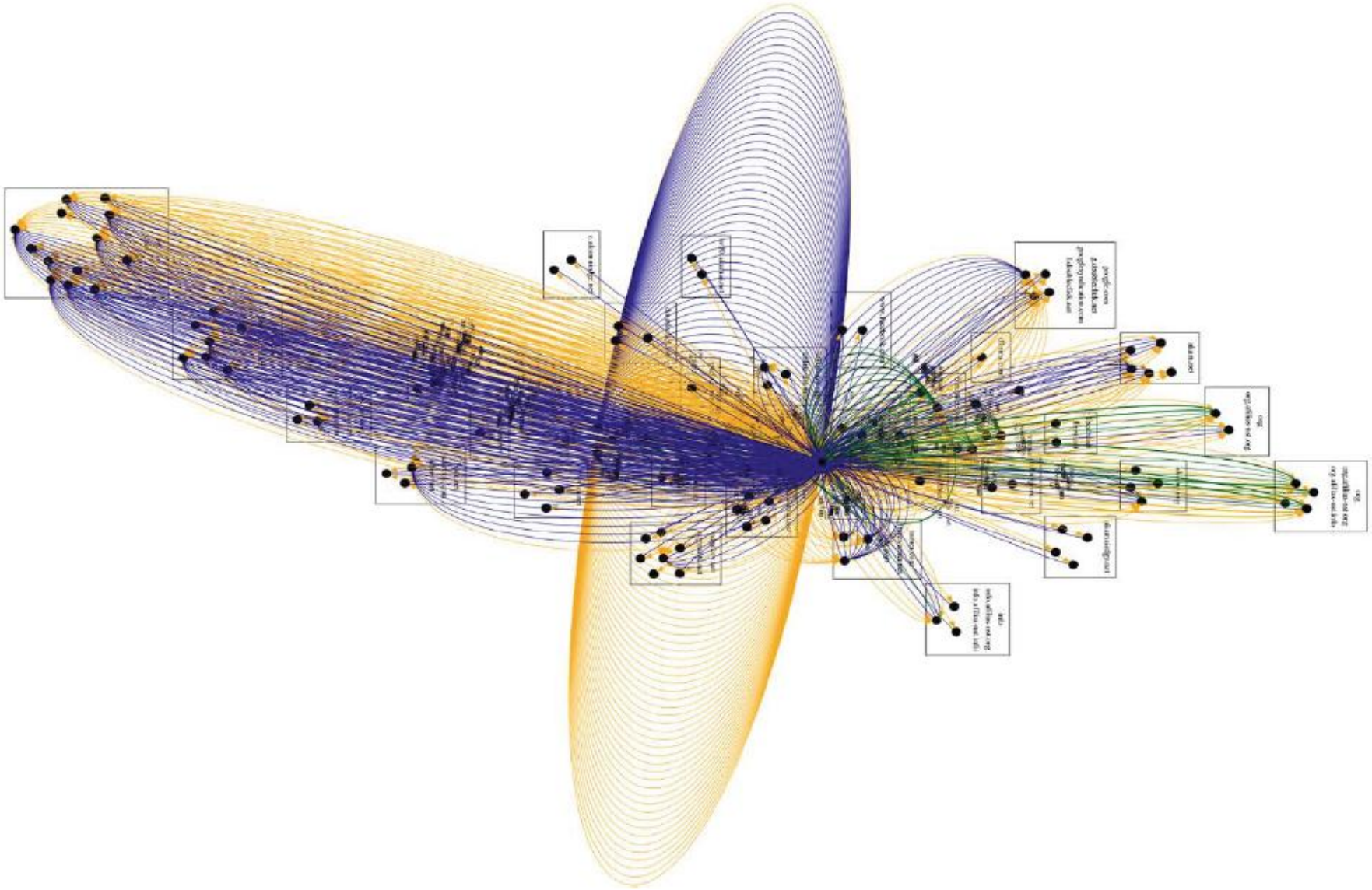
12

On the use of Domain Names

nominet

- Mobile use of the internet changes the use of domain names significantly
- Mobile Apps provide a direct interface, instead of a web-interface
- Though not obvious, it still requires DNS
- DNS traffic growth rate is increasing
- Many more devices per household
- Many more links per webpage
- pre-fetching in browsers
- With the rise of DNS traffic, there is a rise of attack vectors.

www.cnn.com



New avenues in DNS

nominet

- DNS-based Authentication of Named Entities
- Expected to replace Certificates eventually
- Depends on the deployment of DNSSEC
- Depends on the cooperation of application vendors