

Resilience improving features of MPLS, IPv6 and DNSSEC

Sotiris Ioannidis

Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas (FORTH)

Crete, Greece

MPLS, IPv6 and DNSSEC

<http://dcs.ics.forth.gr>

- MPLS
 - Packet relaying
- IPv6
 - Addressing
- DNSSEC
 - Name resolution security

IPv6 Basics

<http://dcs.ics.forth.gr>

- Internet protocol - for packet-switched networks
- Designated successor of IPv4
- Designed to overcome shortcomings and barriers of IPv4
 - Scalability, complexity
 - Security (sort of)
 - Address exhaustion

IPv6 Key Features (1/2)

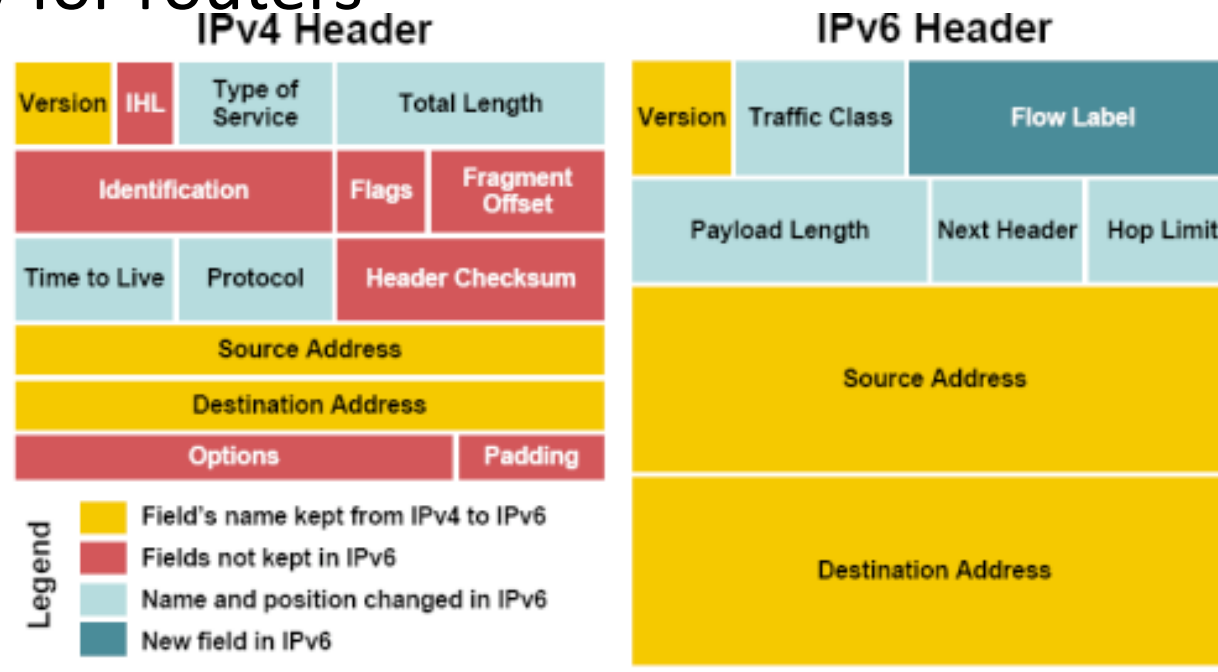
<http://dcs.ics.forth.gr>

- Very large address space
 - 2^{128} possible addresses
- Mandatory support for IPsec in the stack
- Fixed size packet header
- Auto-configuration
- Jumbograms
- Option extensibility
- No fragmentation
- Routing header

IPv6 Key Features (2/2)

<http://dcs.ics.forth.gr>

- Address scopes
 - unicast, multicast, anycast
- Simplified packet header
 - Easy for routers



IPv6 Helpful Features

<http://dcs.ics.forth.gr>

- Large address space thwarts reconnaissance
 - Locating targets through random scanning will not be easy
- IPsec can provide the needed e2e security that we lack today
 - PKI solution is needed
- Everything addressable (no NAT)
 - Fewer statefull nodes
 - Fewer “single points of failure”
- No fragmentation inside the network
 - Remove (some) complexity from the net

IPv6 not so Helpful

<http://dcs.ics.forth.gr>

- Problems with monitoring due to large AS
 - Harder to do telescopes, honeypots, malware uses target list
- Everything addressable
 - Exposes weak hosts, no more hiding behind NAT
- Tracing due to use of MAC in addresses
 - Must randomize MAC
- Transition will be tricky
 - Coexistence of IPv4 and IPv6 may lead to problems

Some challenges still remain

<http://dcs.ics.forth.gr>

- Flooding attacks
 - DoS & DDoS attacks
- Application level attacks
 - SQL injection, server-side buffer overflows, etc.
- Rogue devices on a network
 - Rogue wireless access points
- Address spoofing, MiM attacks
- What fraction of actual security breaches would really be fixed with IPv6?

IPv6 Deployments

<http://dcs.ics.forth.gr>

- Hard to measure, a lot is tunneled over IPv4
 - Count IPv6 prefixes in routing tables
- 6NET
 - 6NET was a three-year European IST
 - 35 partners from 16 countries
 - Built & operated a native IPv6 network
- 2008 Beijing Olympics
 - Showcase for IPv6

IPv6 Conclusion

<http://dcs.ics.forth.gr>

- IPv6 shouldn't be considered an “all-inclusive” resilience/security solution
- Main reason for changing from IPv4 to IPv6 is the larger address space, not some fundamental security features
 - Apparently operator survey also points to this

MPLS Basics

<http://dcs.ics.forth.gr>

- Packets are forwarded based on a (stack of) labels with per-link scope. Labels are distributed with the help of a variety of control protocols.
- MPLS is typically used to implement:
 - L2 p2p connections (pseudo-wires) that can carry legacy traffic (ATM, Frame Relay). In these cases MPLS can be viewed as a replacement of these legacy technologies
 - Various types of VPNs (L2 and L3 VPNs). In this case MPLS implements both new functionality and replaces existing functionality in the network.
 - Force traffic to follow certain engineered paths (traffic engineering). In this case MPLS is used to implement new functionality in the network.
 - Recover fast (sub 50 msec) from link and node failures. In this case MPLS is used to implement new functionality in the network.

MPLS Analysis

<http://dcs.ics.forth.gr>

- MPLS allows operators and network service providers to offer a variety of services on top of a single converged and low cost platform
 - Consolidating multiple technologies (ATM, FR) and networks into a single easier to run network.
- Using MPLS has impact on both the security and the resiliency of the network
 - Mechanisms that increase the resiliency to network failures or to sudden variations in traffic patterns and load (traffic engineering).

MPLS Helpful Features (1/3)

<http://dcs.ics.forth.gr>

- Class of Service (CoS)
 - The CoS feature for MPLS enables network administrators to provide differentiated services
 - Packets are marked according to the service requested
 - CoS offers:
 - packet classification
 - congestion avoidance
 - congestion management

MPLS Helpful Features (2/3)

<http://dcs.ics.forth.gr>

- Protection Features
 - Protection vs Restoration
 - Path Protection
 - Local Protection
- Protection Modes
 - +1 protection
 - Flow sent on two separate disjoint paths
 - Receiver responsible for choosing one of the two
 - 1:1 protection
 - A backup path protects a single LSP (or a portion of a single LSP)
 - N:1 protection
 - A backup path protects one link or one node or both
 - Overlapping portions of many LSPs are protected by a single backup path
 - Applicable for local protection only
 - N:M protection ($M < N$)

MPLS Helpful Features (3/3)

<http://dcs.ics.forth.gr>

- Security by Hiding the Core (Closed Network)
 - Address Space & Routing Separation
 - Hiding of the MPLS Core Structure
 - Label Spoofing
- Having secured the internals, the attacker can only attack the ingress, egress points of the network.

MPLS Deployments

<http://dcs.ics.forth.gr>

- Bell Canada
- Alcatel – Lucent
- AT&T
- MCI
- BT
- Orange
- Vodafone
- OTENET
- Many more

MPLS Conclusions

<http://dcs.ics.forth.gr>

- Proven, well deployed technology
- WRT security, edges still vulnerable
- Insider attacks

DNSSEC Basics

<http://dcs.ics.forth.gr>

- **DNSSEC** is a set of extensions to DNS for securing certain kinds of information
- It is a cryptographic signing system
 - Uses public key (asymmetric) cryptography and cryptographic hashes.
- DNSSEC is not a security panacea.
 - But it does give us some security guarantees

DNSSEC Helpful Features (1/2)

<http://dcs.ics.forth.gr>

- DNSSEC enables a security–aware receiving name server to:
 - Authenticate that the data received could only have originated from the requested zone
 - Verify the integrity of the data. The data that was received at the querying name server was the data that was sent from the queried name server
 - Verify that if a negative response (NXDOMAIN) was received to a host query, that the target record does not exist (denial of existence)
- A powerful solution to DNS cache poisoning attacks

DNSSEC Helpful Features (2/2)

<http://dcs.ics.forth.gr>

- Prevents (some) Man-in-the-Middle attacks
- Protects clients from forged replies that have been created by an attacker, by exploiting query prediction
- An efficient way to prevent pharming attacks
 - Where hackers try to redirect traffic to a malicious, attacker controlled, website

DNSSEC Possible Limitations (1/2)

<http://dcs.ics.forth.gr>

- Denial of Service attacks
 - DNSSEC authoritative name servers would be marginally more vulnerable to DoS attacks (they send more zone records).
- Answer validation increases the resolver's work load
 - This increased workload will also increase the time it takes to get an answer back to the original DNS client
 - Increase is minor, also crypto costs are minimal
- Trust model hierarchical
 - Each zone parent is given the role of signing over every delegated child's zone key

DNSSEC Possible Limitations (2/2)

<http://dcs.ics.forth.gr>

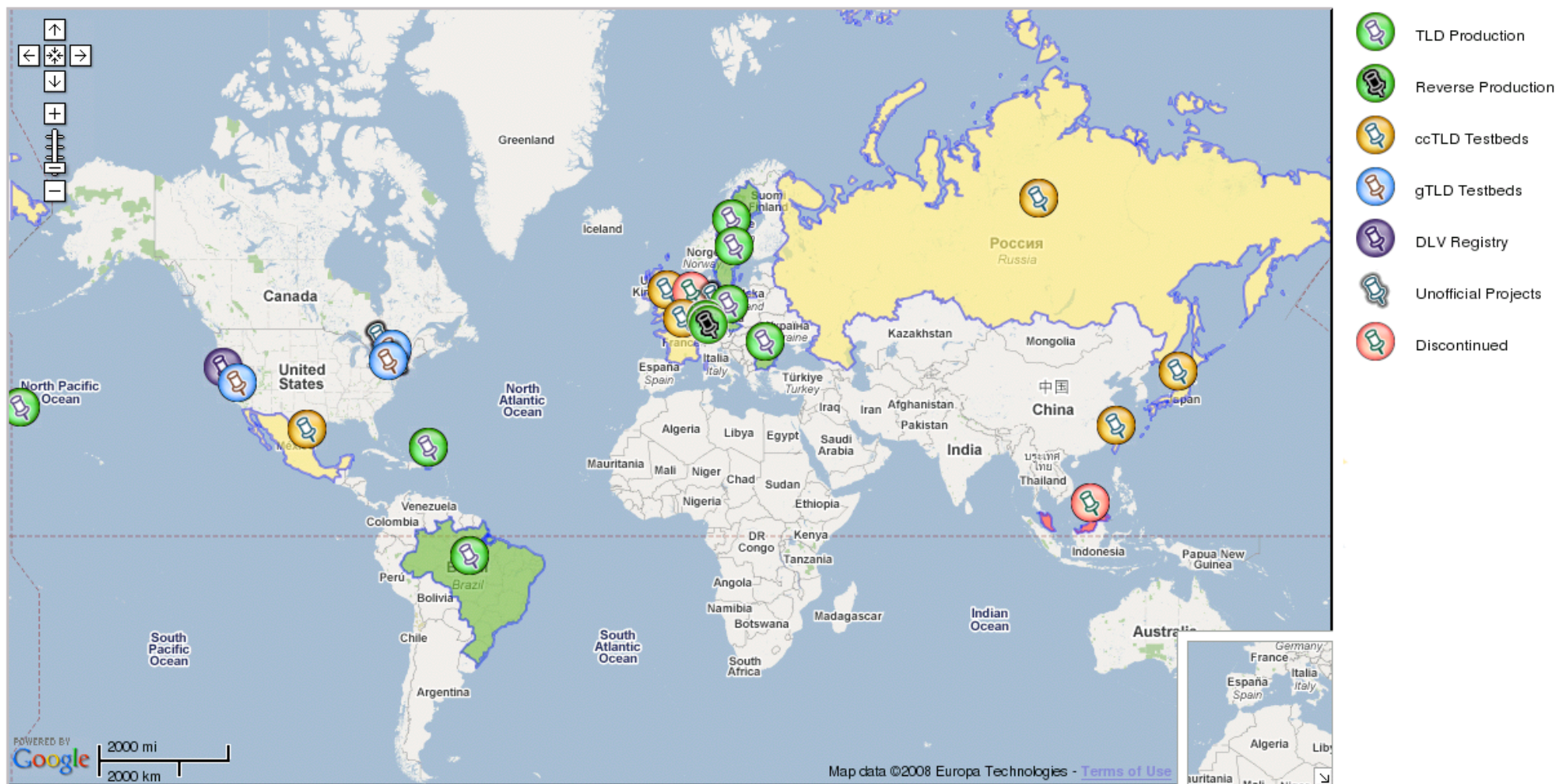
- The average size of a DNS response message increases
 - Due to the additional signature records that are attached to the responses.
- Zone file increases in size
 - The major contributors here are the NSEC and RRSIG resource records
- Key rollover at the root is really hard
 - It affects the whole hierarchical structure
- Key management is always tricky

DNSSEC Deployments

<http://dcs.ics.forth.gr>

- Sweden is the first country in the world that in late 2005 announced the signing of .se ccTLD
- At this time, DNSSEC is also deployed in Brazil (.br), Czech Republic (.cz), Puerto Rico (.pr) and Bulgaria (.bg)
- Future deployments include .org, .gov zones and the **root zone**

DNSSEC Deployments



DNSSEC Conclusions

<http://dcs.ics.forth.gr>

- If deployed and used properly it will eliminate a certain class of attacks
- Main challenge is key management

Conclusions

<http://dcs.ics.forth.gr>

- All three technologies have useful features that could affect the resiliency of the network
- However, resiliency is about more than just cobbling together technologies
- It is important to understand what each technology buys us
- Report to ENISA mid-December

Backup slides

<http://dcs.ics.forth.gr>

DNSSEC Analysis

<http://dcs.ics.forth.gr>

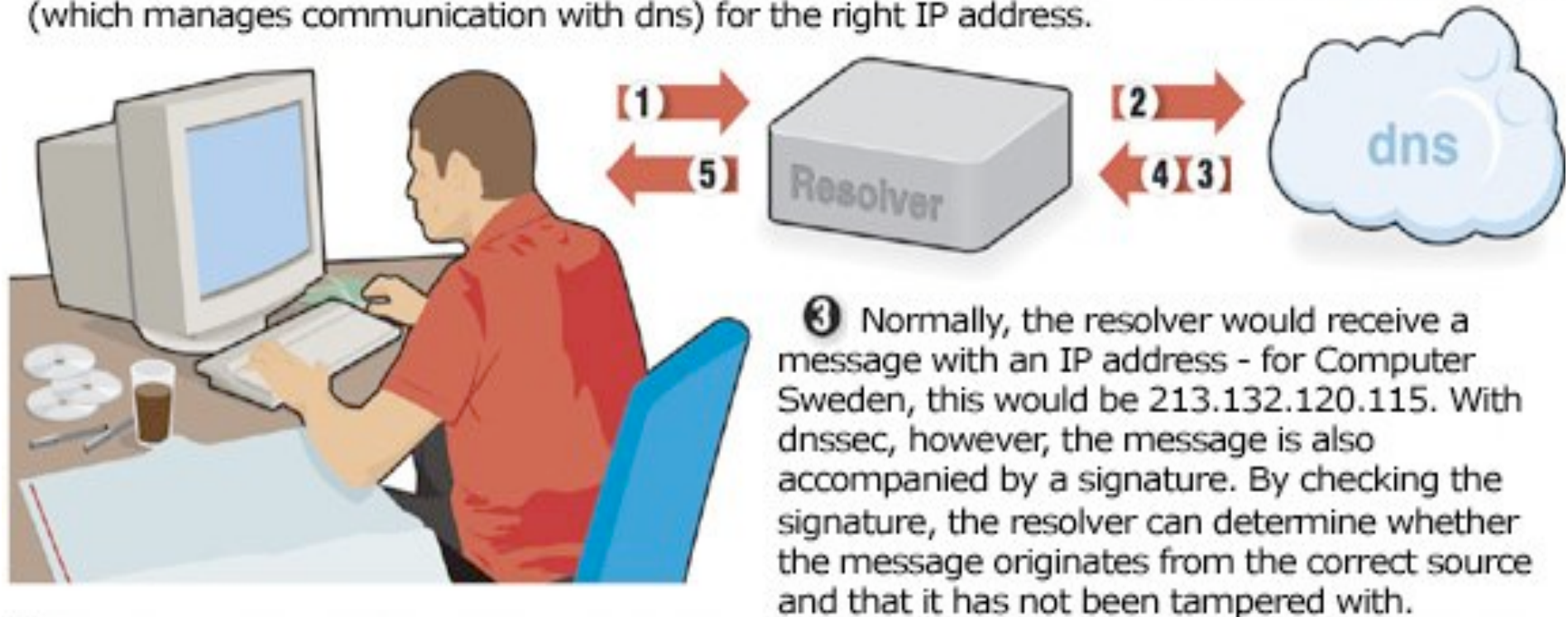
- Introduces special sets of Resource Records
 - DNSKEY: the public key of a zone – the zone is digitally signed using the private key of a key pair.
 - RRSIG: RRsets are digitally signed by the zone administrator – each RRset would have its own RRSIG RR.
 - NSEC/NSEC3: chain together the valid host names appearing in the zone file – authenticate "denial of existence" of a DNS query.
 - DS: a secured zone can be added to an existing chain of trust or can be used to secure delegation to a sub-domain
 - contains the hash of the DNSKEY RR, that lives in the secured child zone.

In a Nutshell

<http://dcs.ics.forth.gr>

1 The web surfer keys in computersweden.se in his/her web browser. The web browser submits a query to the resolver (which manages communication with dns) for the right IP address.

2 The resolver forwards the address query to dns.



3 Normally, the resolver would receive a message with an IP address - for Computer Sweden, this would be 213.132.120.115. With dnssec, however, the message is also accompanied by a signature. By checking the signature, the resolver can determine whether the message originates from the correct source and that it has not been tampered with.

4 The resolver must also check that the signature has been created with the right key. This is done by following the "chain of trust", which in this case goes to the .se domain root server.

5 Finally, the approved IP address is sent to the web surfer.