Resilience improving features of MPLS, IPv6 and DNSSEC

Sotiris Ioannidis
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece

 sotiris@ics.forth.gr

MPLS, IPv6 and DNSSEC

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

sotiris@ics.forth.gr

IPv6 Basics

- 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

sotiris@ics.forth.gr

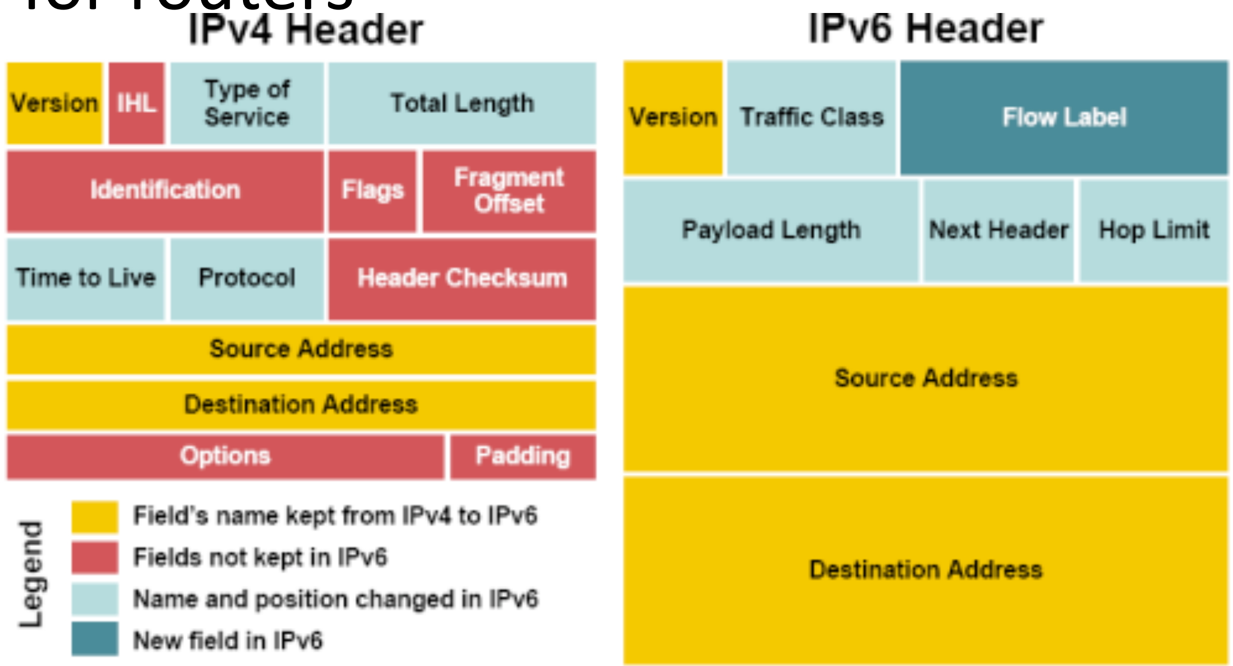
IPv6 Key Features (1/2)

- 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

sotiris@ics.forth.gr

IPv6 Key Features (2/2)

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



IPv6 Helpful Features

- 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

- 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

- 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

- 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

- 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

sotiris@ics.forth.gr

MPLS Basics

- 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.

sotiris@ics.forth.gr

MPLS Analysis

- 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)

- 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

sotiris@ics.forth.gr

MPLS Helpful Features (2/3)

- 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)

- 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

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

MPLS Conclusions

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

 sotiris@ics.forth.gr

DNSSEC Basics

- **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)

- 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)

- 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)

- 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)

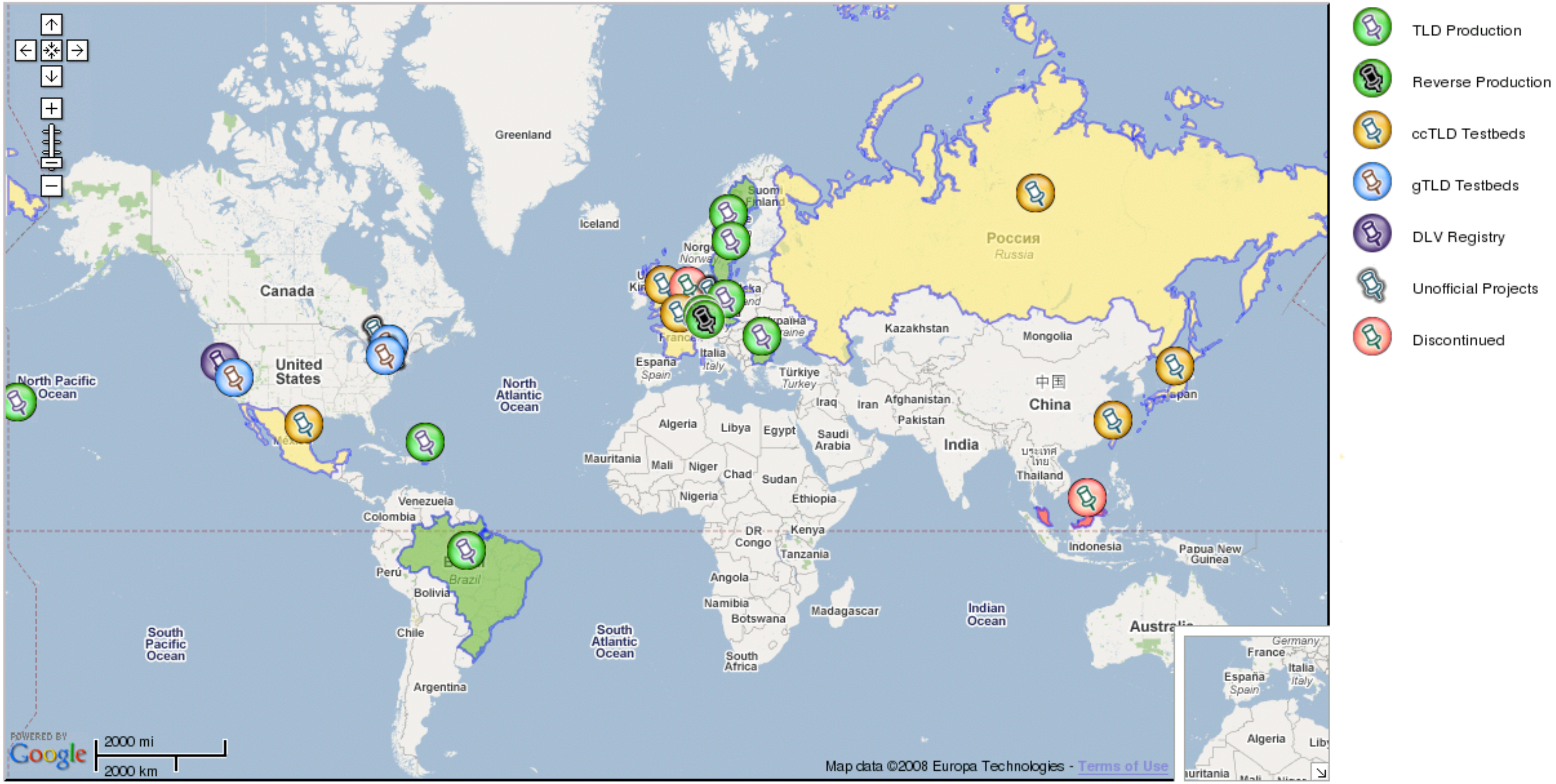
- The average size of a DNS response message increases
  - Due to the additional signature records that are attached to the responses.
- Zone file increases in size
  - The major contributors here are the NSEC and RRSIG resource records
- Key rollover at the root is really hard
  - It affects the whole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

DNSSEC Deployments

- 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**

sotiris@ics.forth.gr

DNSSEC Deployments



DNSSEC Conclusions

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

Conclusions

- 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