Economical and Political Implications of DNSSEC Deployment

AXEL FANT-ELDH
and
MATTIAS KIRVESNIEMI

KTH Information and
Communication Technology

Bachelor of Science Thesis
Stockholm, Sweden 2010

TRITA-ICT-EX-2010:108

School of Information and Communication Technology

Royal Institute of Technology (KTH)

Economical and Political Implications of DNSSEC Deployment

Bachelor thesis

Axel Fant-Eldh
Industrial Economics,
Royal Institute of Technology,
Stockholm
axelfe@kth.se

Mattias Kirvesniemi
Industrial Economics,
Royal Institute of Technology,
Stockholm
mkir@kth.se

Examiner:
Gerald Q. Maguire Jr.
maguire@kth.se

5/27/2010

Abstract

This report provides a summary of the current deployment of Domain Name System (DNS) Security Extensions (DNSSEC) as well as a discussion of future deployments and deployment rates. It analyses the problems that have occurred and considers those that may arise. This thesis focuses mainly on economical and political perspectives, rather than the technical perspective used in most reports regarding this subject.

There were four areas that needed to be examined: the technical basis for DNSSEC, the deployment process, the current level of DNSSEC deployment, and the opinions regarding this subject. The information about the deployment process was obtained mainly through articles, but also through reports from organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Electronic Privacy Information Centre. To acquire up to date data on DNSSEC deployment, SecSpider was used to research the level of deployment as of 2010-05-06. The search was restricted to the generic Top Level Domains (gTLDs) and country code TLDs (ccTLDs) of the top 20 countries in terms of Internet usage as well as the OECD countries. This restriction was made to narrow down the scope to the TLDs where DNSSEC would have the greatest impact. The "Top 20" comprises 77.27 % of the world's Internet users, hence it is where DNSSEC deployment would affect the most people. The OECD is in this thesis considered a sufficiently large selection to represent the most technologically advanced and economically powerful countries in the world regardless of size. Major powers such as China, India, and Russia while not included in the OECD are represented in the "Top 20" due to their size.

Our results show that some major TLDs have implemented DNSSEC and that the rate of deployment has increased in the last few years. However, the level of DNSSEC deployment in the TLDs is still rather low; 15.00 % in the gTLDs and ccTLDs of the Top 20 countries in Internet usage, and 20.00 % in the OECD's ccTLDs. Deployment in the root is ongoing during spring 2010, this could have a great impact on the rate of deployment as deployment in a gTLD or ccTLD is highly dependent on deployment high up in the hierarchy due to the nature of DNSSEC. It is unlikely that corporations would implement DNSSEC without a potential return on investment (ROI) and management control measures from governments might be required to increase deployment pace at the lower levels of the DNS hierarchy.

Abstrakt

Denna rapport innehåller en sammanfattning av den nuvarande spridningen av Domain Name System (DNS) Security Extensions (DNSSEC) och även en diskussion om framtida spridning och spridningstakt. Den analyserar problemen som uppstått och avväger de som kan uppstå. Rapporten fokuserar mer på de ekonomiska och politiska perspektiven, snarare än det tekniska som använts i de flesta rapporter inom området.

Det var fyra områden som behövde undersökas: den tekniska basen, spridningsprocessen, nuvarande spridningsnivåer av DNSSEC samt åsikter kring området (om inte DNSSEC adopteras av faktiska användare kommer dess effekt att bli minimal). Informationen angående spridningsprocessen anskaffades huvudsakligen genom artiklar, men även från rapporten utgivet av organisationer likt the Internet Corporation for Assigned Names and Numbers (ICANN) och the Electronic Privacy Information Centre. För att erhålla färsk information på spridningen av DNSSEC undersökte vi spridningsnivån 2010-05-06 med SecSpider. Vi avgränsade vår undersökning till generic Top Level Domains (gTLDs) och country code TLDs (ccTLDs) från de 20 främsta länderna i Internetanvändande samt OECD-länderna. Denna avgränsning gjordes för att fokusera på de TLDs där spridning av DNSSEC skulle ge störst påverkan. ”Topp 20” innehåller 77.27 % av världens Internetanvändare och det är här spridning av DNSSEC skulle nå flest användare. OECD anses i denna rapport vara ett tillräckligt urval för att representera de mest teknologiskt avancerade och ekonomiskt mäktiga ländrena oavsett storlek. Betydande makter såsom Kina, Indien och Ryssland som inte ingår i OECD är inkluderade i ”Topp 20” tack vare sin storlek.

Resultaten visar att några betydande TLDs har implementerat DNSSEC och att spridningstakten har ökat de senaste åren. Dock är spridningsnivån i TLDs fortfarande ganska låg; 15.00 % i gTLDs och ccTLDs i ”Topp 20”, och 20.00 % i OECDs ccTLDs. Implementering i rooten pågår under våren 2010, något som skulle kunna ha stor påverkan på spridningstakten eftersom den är starkt beroende av spridning högt upp i hierarkin på grund av DNSSECs natur. Det är osannolikt att företag skulle implementera DNSSEC utan möjlig avkastning på investerat kapital och ekonomiska styrmedel från regeringar kan behövas för att öka spridningstakten på de lägre nivåerna.

Acknowledgments

We would like to take this opportunity to thank people that have helped us with this bachelor thesis. Foremost we would like to thank our examiner Gerald Q. Maguire Jr. for accepting our selected area and help us getting started. Another person that has helped us a lot is Richard Nordberg, who has helped us with our structure and language.

Special thanks go out to Hans Åkesson and Mats Dufberg at Telia Sonera for their kind help in answering our questions about their company and DNSSEC.

Table of Contents

Table of Figures

List of Acronyms and Abbreviations

AD Bit	Authenticated Data Bit
ADNS	Administrative DNS Servers
CA	Certificate Authority
ccTLD	Country Code TLD
CD Bit	Checking Disable Bit
DNS	Dynamic Name System
DNSSEC	Dynamic Name System Security Extensions
EDNS0	Extension mechanisms for DNS, required for DNSSEC
gTLD	Generic TLD
IP	Internet Protocol
ISP	Internet Service Provider
KSK	Key Signing Key
LDNS	Local DNS Servers
NXT	Next
PK-DNSSEC	Public Key DNSSEC
ROI	Return On Investment
RR	Resource Record
RRset	Resource Record Set
SIG RR	Signature Resource Record
SK-DNSSEC	Secret Key DNSSEC
TAR	Trusted Anchor Repositories
TLD	Top Level Domain
TTP	Trusted Third Party
URL	Uniform Resource Locator
ZSK	Zone Signing Key

1. Background

There is an ongoing expansion of the Internet and its applications. People around the world practically live their lives on the Internet, through different communities, paying their bills, working from home, and so on. With this expansion of use, increasing amounts of sensitive material and information are becoming available on the web; hence there is a growing concern that people can get hold of this information and use it for personal gain or other malicious purposes.

One of the ways this information can be obtained is through the Dynamic Name System (DNS) protocol. DNS is a central part of Internet usage, but is underdeveloped, which allows it to be used for attacks by malicious interests. In order to address these attacks the Dynamic Name System Security Extension (DNSSEC) was created [1]. The deployment of DNSSEC and the economical and political implications of it are the main foci of this paper. The research will examine deployment within the Organization for Economic Co-operation and Development (OECD) and the major Internet using countries, which support most of the Internet users and their traffic. Within these countries both the benefits and complications of the deployment of DNSSEC will be analyzed and discussed. This will provide complementary information to the existing research that has focused on the technical aspect of DNSSEC in depth.

2. DNSSEC

To understand the concept of DNSSEC the basics of DNS will be explained. The main purpose of DNS is to simplify Internet usage for ordinary users with little or no knowledge of Internet Protocol (IP) addressing. DNS enables the translation of a Uniform Resource Locator (URL) typed into the user's Internet browser, through DNS look-ups, to an IP address. The browser then establishes communication based upon this IP address. The DNS look-ups are transmitted throughout the hierarchal DNS server infrastructure, which is a tree structure comprised of Local DNS servers (LDNS), Authoritative DNS servers (ADNS), and root servers. With the existing server settings there are two big security problems: (1) DNS spoofing (an attacker manipulates the DNS answer) and (2) DNS poisoning (faulty data enters the server cache); DNSSEC provides a solution to these problems [2].

The primary objective for DNSSEC is to provide authentication and integrity for the data received from DNS servers. This authentication and integrity is achieved through digital signatures based on public key cryptography [1]. The associations between keys and DNS names are stored in a Resource Record (RR) format. When there are several RRs of the same type, they defined a Resource Record set (RRset). A RRset is authenticated by a signature (SIG) RR that is impossible to forge, due a the chain of trust for this signature. A chain of trust is when a zone (child zone) trusts the zone above it in the hierarchy (parent zone) and the zones beneath it (child's child zones) can trust it. This creates implicated trust between the parent and underlying zone/zones of the child (see Figure 1). The SIG RR also binds the RRset to a time interval (during which this signature will be valid) and the SIG RR's domain

name [2]. SIG RRs are used when DNS answers queries by adding the corresponding signature for each RRset and making sure to include the entire RRset in order to enable verification by the resolver. These queries and answers allocate two bits from the DNS format header to authenticate data (the authentic data [AD] bit) and to indicate if the resolver sending the query accepts pending (non-authenticated) data (the checking disable [CD] bit) [1].

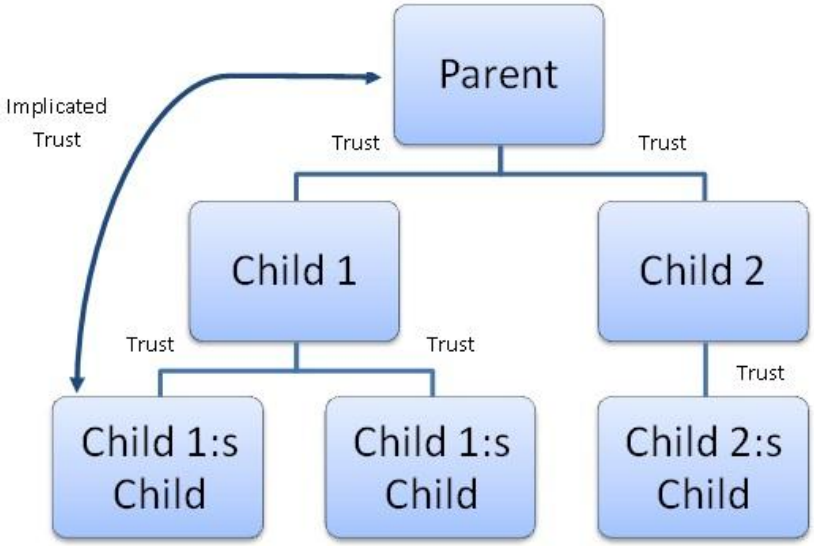


Figure 1 - Chain of Trust

It is also necessary to use "next" (NXT) RRs, which are associated with domain names and their correlating RRs. These NXT RRs indicates which domain name is next in canonical order. There was an early problem with NXT where the last NXT RR in a zone could not point to the next NXT. This was solved by putting the first RR next to it, creating a circle. In the event that a resolver queries for a non-existent domain name or data type it receives a SIG RR covered NXT RR. This NXT gives the resolver a record of which domain names and RRs are available, to avoid generating signatures for non-existent statements. Due to this circular structure an attacker can make a query from a domain name for the NXT record, hence learning the next domain name in canonical order. This process can be repeated to learn all domain names in a zone [2]. This means that the existence of a domain name record is not itself secret.

During the implementation of DNSSEC a major problem occurred, which caused some zones to be unreachable for other zones that tried to enter through a parent zone [3]. This problem only occurred when a child zone was not DNSSEC compatible while the parent zone was. When the parent tried to create a secure chain of trust the child zone did not understand the message and disregarded it (see Figure 2). This resulted in the parent being unaware of the existing child's zone and no information could reach it. To solve this problem a modification to the protocol was made. This made it possible for routers to enable or disable DNSSEC depending on the source's and destination's compatibility. If one or the other is not compatible with DNSSEC, then the requirement for DNSSEC would be turned off so that ordinary DNS could be used to transmit the information [3].

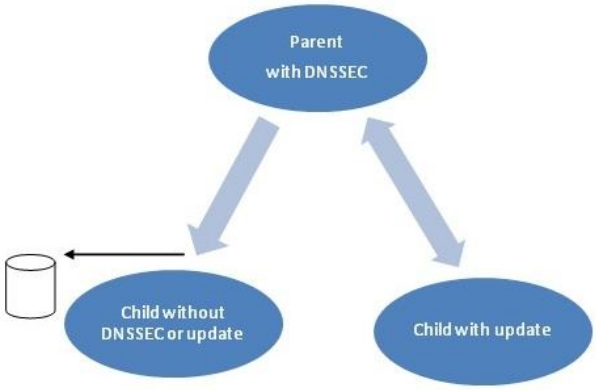


Figure 2 - DNSSEC Compatibility Issues

2.1 TAR's

In order to get the chain of trust that is needed in DNSSEC, a resolver must be certain that a root key can be explicitly trusted, this is called a trusted anchor. A Trusted Anchor Repositories (TAR) was created since the root servers were initially not compatible with DNSSEC. These TARs were assigned to holding the trust anchor of multiple zones. This makes it possible for ADNS and LDNS to use the benefits of DNSSEC even while the root was not signed.

Key Signing Keys (KSKs) are generated by TARs. These KSKs are then used to create a Zone Signing Key (ZSK) for each level, which is used for signing the underlying zone. A KSK for the desired zone is created with the ZSK from the parent zone. Every parent zone stores the hash of every child's KSK in their DNSKEY RR. This empathizes the trust in that key (see Figure 3). This procedure of using a KSK to generate a ZSK is repeated until the requested zone is reached and secured [4].

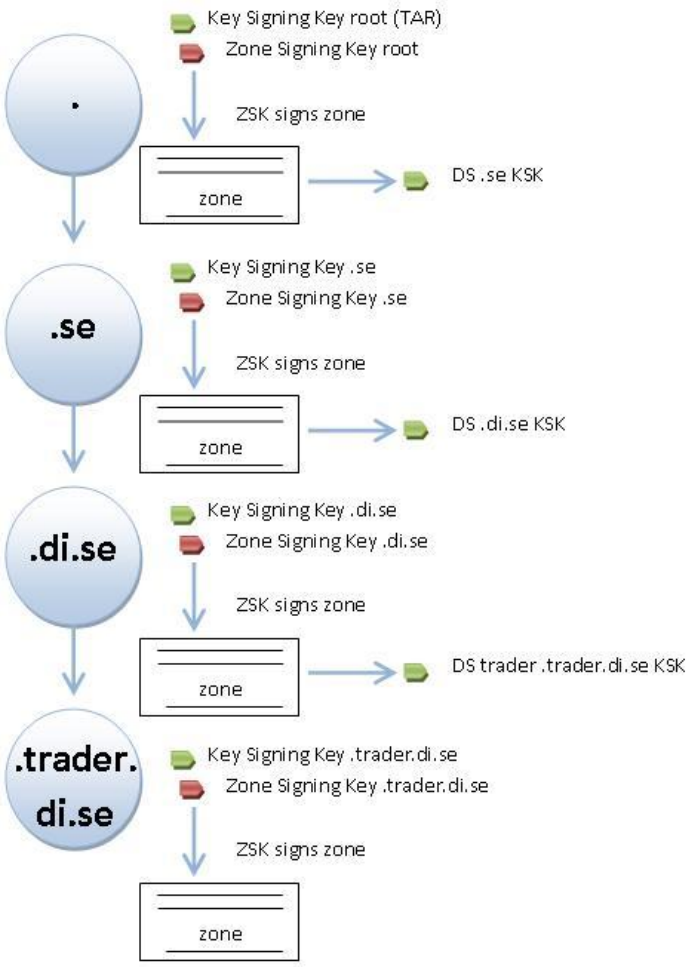


Figure 3 –Key signing with TAR

2.2 Key sizes

A big problem with DNSSEC is that it can increase latency for the consumers. They must now not only wait for the resolver to resolve a domain name into an IP address, but also wait for the transfer of additional data and the time required to do the authentication and integrity checks associated with these messages. To solve this public concern studies have been made on how key sizes in DNSSEC are related to speed of DNS resolution by users' Internet Service Providers (ISPs) [2]. At first big keys were used due to the logical reasoning that more information sent would provide higher speed and most importantly higher security. This did not turn out to be the solution to the problem of latency. Using large packets means that if a packet is lost, then there is more information that needs to be resent. This problem also emerges if the Time To Live (TTL) for a packet expires. So in order to minimize the required bandwidth the protocol implemented by ISPs will probably use small keys.

2.3 Secret Key DNSSEC

Giuseppe Ateniese and Stefan Mangard have developed a new approach to DNS security, Secret Key DNSSEC (SK-DNSSEC) [2]. While "regular" DNSSEC uses public key cryptography (PK-DNSSEC), Ateniese and Mangard mostly employ symmetric (or secret key) cryptography to efficiently build a chain of trust between a DNS root and the authoritative server. A symmetric certificate connects the user identity to a secret key generated using symmetric cryptographic techniques. An advantage of using symmetric cryptography is that it is much faster than public key cryptography.

The authentication required for any public key cryptography is usually provided via trusted certification authorities (CAs) [2]. PK-DNSSEC is in some cases more practical, as the Trusted Third Party (TTP) only has to be functional and is not required to be active during secure transactions; while in contrast SK-DNSSEC requires the TTP to be operated online. Additionally, in some cases PK-DNSSEC does not require the TTP to be unconditionally trusted because it does not have access to the secret keys corresponding to the public keys (in fact all it has to do is deliver public certificates). However, in the case of certified public keys the CA (the TTP) could generate a false certificate and read encrypted messages or sign arbitrary messages under the stolen identity, thus it must be fully trusted. In contrast, SK-DNSSEC requires the TTP to be unconditionally trusted and constantly online, in practice this requires that the secret key algorithms are very fast and that the keys are relatively short. These short keys will lead to higher performance for the end consumers, which makes this DNSSEC solution more value creating than the original.

PK-DNSSEC works by building the chain of trust from the root to the authoritative server and every node it passes through acts as a CA for its children. The information retrieved from the DNS database is signed by the DNS servers and has to be unconditionally trusted. Ateniese and Mangard deduce from two key factors that the network configuration and trust model of PK-DNSSEC would not change if SK-DNSSEC were employed instead:

1. that DNS is active in any request
2. that the information retrieved from the database is signed by name servers.

They believe that this should greatly ease the implementation of SK-DNSSEC, as it could be done seamlessly in parallel to PK-DNSSEC.

According to Ateniese and Mangard SK-DNSSEC provides advantages over PK-DNSSEC in terms of higher performance, reduced network traffic, less storage, and robustness to replay attacks, while providing mutual authentication and confidentiality [2].

3. Current Situation

According to a survey over 65 country code Top Level Domains (ccTLDs) used by Paul Wouters in October 27th 2007 [5], 7 % had implemented DNSSEC. Among those who had not, 85 % intended to sometime in the future. The reason for the delay was in most cases lack of resources or that they did not consider DNSSEC mature enough yet. Over 70 % intended to implement DNSSEC within 3 years.

The maturity concerns could be compounded by the fact that when DNSSEC was deployed on a large scale in Sweden it broke the connectivity for many users [5]. The cause was cheap routers that could not handle the AD bit properly and dropped the packets. A solution was not hard to achieve, some routers just needed a software update and others that where too old for that update needed to be replaced. Because of high age of the replaced routers it was a relatively low cost to replace them, since they were close to or had exceeded their economical lifetime expectancy. This means that the economical value of these old routers was close to or actually zero.

As poisoning attacks have hit major targets, DNS security concerns have risen significantly. This has resulted in increased calls for a wider and more rapid deployment of DNSSEC [6]. All types of entities have apply pressure, from governments all the way down to private consumers. Everyone with some kind of sensitive information on the Internet wants to make sure that no one with malicious interests is able to obtain that information or is able to persuade someone else that they are actually communicating with the correct entity – when they are in fact communicating with an imposter.

4. Research

As described earlier there were four areas that needed to be researched: the technical base, the deployment process, the current level of DNSSEC deployment, and the opinions regarding the subject. The technical base provides an understanding of the benefits and the functionality of DNSSEC. Reports on the deployment process will provide information about the implications from deployments that have occurred so far. The current level of deployment is relevant in two ways: (1) first and foremost it shows how far the deployment has come and how much there is to be done and (2) where the deployment has occurred. The opinions provide a view of the climate surrounding the subject.

4.1 Methods

The technical research was mainly done through Google scholar and with emphasis on finding recent articles that still were relevant. The contents of the technical articles were distilled to focus on the functionality and benefits as the technical details were omitted due to focus of the thesis. In an attempt to quantify the latency added by DNSSEC a DNS benchmarking tool was used to acquire data on DNS performance with and without DNSSEC authentication. This data was then analyzed using Excel spreadsheets.

The information on the deployment process was obtained mainly through articles, but also through reports from organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Electronic Privacy Information Centre.

To acquire up to date data on DNSSEC deployment, SecSpider was used to research the level of deployment as of 2010-05-06. The search was restricted to the generic Top Level Domains (gTLDs) and country code TLDs (ccTLDs) of the top 20 countries in terms of Internet usage as well as the OECD countries. This restriction was made to narrow down the scope to the TLDs where DNSSEC would have the greatest impact. The "Top 20" comprises 77.27 % of the world's Internet users, hence it is where DNSSEC deployment would affect the most people. The OECD is in this thesis considered a sufficiently large selection to represent the most technologically advanced and economically powerful countries in the world regardless of size. Major powers such as China, India, and Russia while not included in the OECD are represented in the "Top 20" due to their size. An Excel-spreadsheet, where the TLDs were listed, was used to monitor the research results.

The data was put into tables and pivot-tables thus mapping the deployment of Extension mechanisms for DNS (EDNS0, a requirement for DNSSEC deployment) and DNSSEC. These were used to produce percentage statistics, circle diagrams and present the data in a clear visual manner. Reference data such as number of users was gathered from Internet world statistics [7].

Opinions regarding the subject were gathered from a wide arrange of sources: interviews (both those published on the Internet and conducted by ourselves), articles and news reports.

4.2 SecSpider

SecSpider is a tool for monitoring DNSSEC. This tool has been operational for over three years. The purpose of this tool is "to discover and address challenges faced by both the operators of secure DNS zones and the operators of secure resolvers" [9]. SecSpider identifies whether a zone is DNSSEC-enabled or not and can also discover DNSSEC-related issues. For example, SecSpider was the first to discover the Path Maximum Transmission Unit problems that could occur if the size of a DNS-key was too big, as in this case the DNS responses would be lost. SecSpider has assembled the addresses of the zones using different methods, some of this information has been provided by user contributions, while other information has been found using commercial search engines. While the major zones are represented the library, the list is far from complete.

SecSpider has also identified "Islands of Security", basically secure subtrees within the DNS hierarchy. These islands are only really useful if the chain of trust reaches all the way up to the root. While traffic within the island is secure, traffic reaching it from above is not. However, these islands are very useful for mapping DNSSEC deployment, as well as identifying where further deployment would be of most use. Full deployment of DNSSEC would mean only one secure island existed that contains all zones.

4.3 Results

As 2010-05-06 all of the TLDs were EDNS0 capable. However DNSSEC was only deployed in 15.00 % of the gTLDs and the Top 20 ccTLDs (see Figure 4, Table 1, and Table 2). Only 20.00 % of the OECD ccTLDs had DNSSEC deployment (see Figure 5 and Table 3). The higher rate of deployment in the OECD was expected due to the higher rates of Internet penetration as well as the socio-economic status of users in these countries. The only DNSSEC-positive (i.e., an adopter of DNSSEC) zone outside of the OECD in the Top 20 was Brazil (.br). While these numbers seem low, the countries where DNSSEC was deployed contain 21.25% of the world's Internet users (see Table 4) and among the gTLDs were major gTLDs, including .gov and .org. The survey used by Paul Wouters claimed that 70% of those surveyed intended to implement DNSSEC within three years. Unfortunately with only five months before this deadline we conclude that this target will not be achieved.

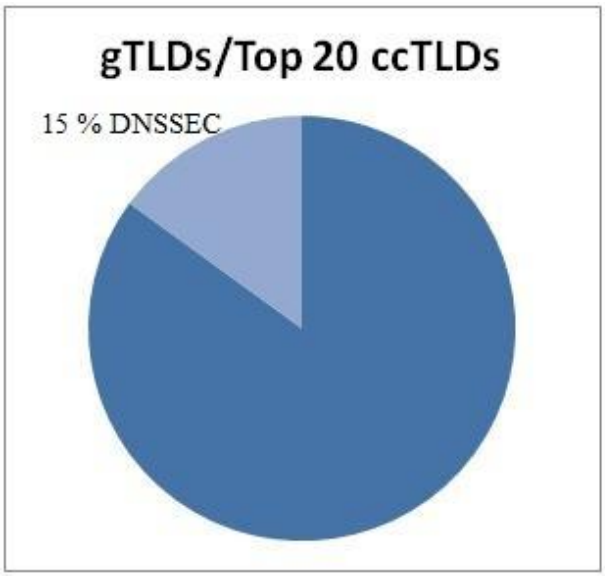


Figure 4 – Level of DNSSEC deployment in gTLDs and Top 20 ccTLDs (indicated by light blue)

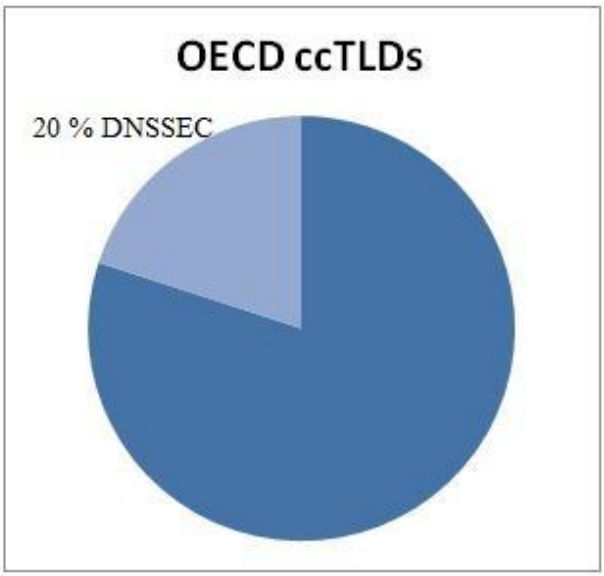


Figure 5 – Level of DNSSEC deployment in OECD ccTLDs (indicated by light blue)

There have been reports that the biggest hurdle in commercial adoption is incentive. Many do not see the benefits and doubt the return on investment (ROI) will be satisfactory. In Sweden, only 14 % of the TLD owners saw DNSSEC as a very interesting commercial service [10].

The results from the benchmarking program showed that there is little latency added when looking up a cached name and while the average lookup times were not much slower in the other cases the standard deviation and maximum time were quite high (see Figure 6).

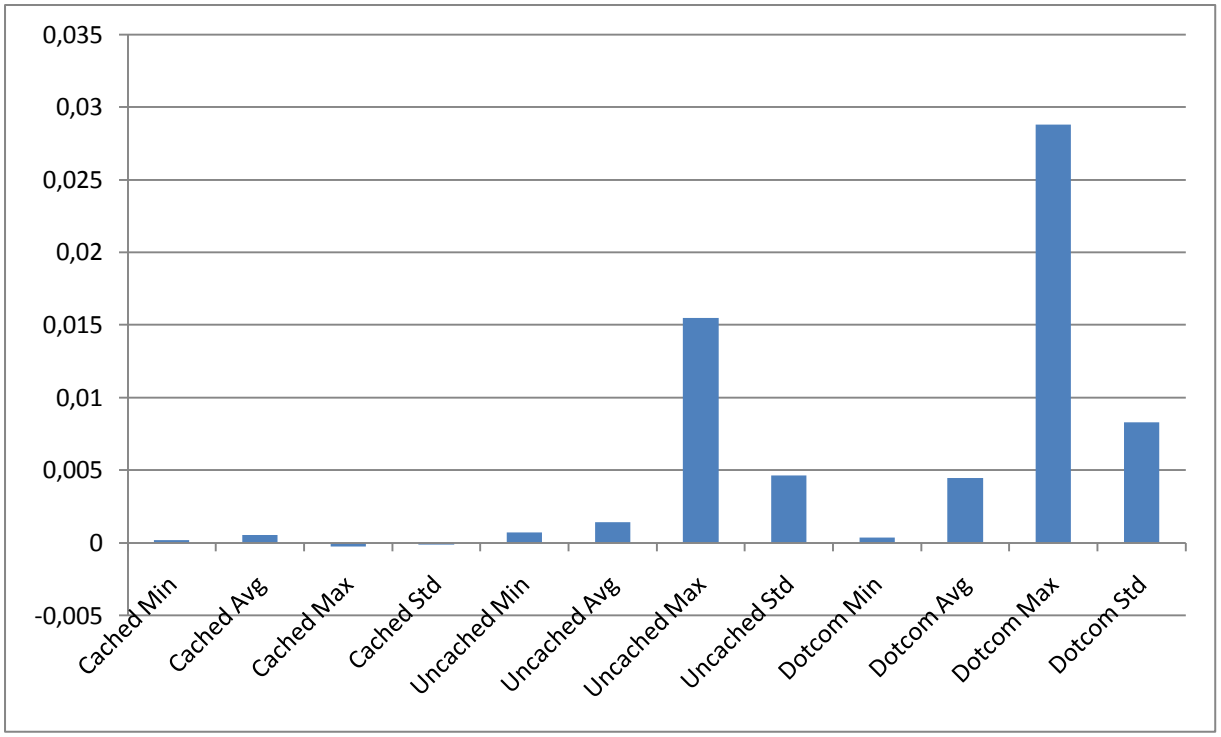


Figure 6 - Added Latency from DNSSEC Authentication (averaged data from 10 nameservers)

Other research [11] shows a performance decrease from DNSSEC of only 2 % using BIND.

5. Stakeholder Analysis

The rate of deployment is dependent upon the stakeholders, therefore the major stakeholders and their interests regarding DNSSEC and other DNS security solutions were analyzed. The most important part of a stakeholder analysis is to select groups that are heavily connected to the subject. With governments being the highest authorities who have the ability to stop or speed up any national development, they are a natural choice. In order to achieve a high degree of DNSSEC penetration without a lot of government funding it is important that corporations find DNSSEC valuable enough to warrant its implementation. The usefulness of DNSSEC to a corporation is highly dependent on the expected ROI and it is important that this investment generate value for their customers and provide a bigger market share or increased profit margin. When discussing ROI it is important to not only consider the obvious returns such as income or market shares and look at alternative costs in potential loss of market share and intangible benefits such as goodwill and image.

5.1 Governments

According to Thierry Moreau governments might be opposed to the spread of DNSSEC, as it could give support to other security schemes [12]. These could conceal information, which goes against "national security interests" (i.e. monitoring Internet activity to keep an eye on malicious interests). As many active participants in DNS Extensions work for organizations closely connected to OECD governments this could have negative consequences for the deployment of DNSSEC according to Moreau. He probably considers the OECD governments to be the ones most concerned with "national security interests" and that they would lobby against the deployment of DNSSEC.

The research reveals that the deployment of DNSSEC was higher among the OECD than the Top 20. The likely reason for this is while many of the OECD countries have a lower absolute numbers of users, the Internet penetration is higher among the OECD making DNSSEC deployment a more relevant issue. However, the countries that come to mind when discussing "national security interests"; the US and the UK, both had DNSSEC deployed in their ccTLDs and in the .gov and .org gTLDs. Another example is Sweden where Internet surveillance has been a hot topic the last few years. The Swedish TLD (.se) was first to deploy DNSSEC in February 2007 and according to Telia the government encourages corporations to implement it [13] [14]. This seemingly disproves Moreau's hypothesis.

If a government decides to create a national environment that supports implementation of DNSSEC, they give financial aid to corporations that implement it. Through this management control measure corporations would have more incentive to apply DNSSEC to their systems. The target for a government should be to achieve complete national deployment of DNSSEC, since the effectiveness of the protocol is proportional to the degree of deployment.

In order to increase security at TLDs DNSSEC must be implemented at the root server. There were differing opinions on who should guard the master key which was a problem [10]. The US Government's Department of Homeland Security wanted to manage the master key, this was viewed by many as not appropriate because they have an interest in doing what is best for their own country. In the end ICANN was granted the authority over the master key and

implementing DNSSEC at the root level, maintenance of the system was awarded to VeriSign [15]. The deployment process is well underway (spring 2010) and the estimated date of completion is July 15th.

5.2 Corporations

Larger corporations using a private name server could benefit from DNSSEC as it could give them system-wide security while requiring only a rather simple implementation. Such an implementation would clearly be of major interest for Internet banks and e-commerce site due to financial transactions, as DNSSEC could reduce doubts that might inhibit consumers from using their services. This desire to increase trust would be similar for most government organizations.

Other groups that are involved in the process of applying DNSSEC throughout their systems are ISPs. ISPs have to deal with all the implementation problems throughout the system, which makes these companies the best contributors toward a full DNSSEC implementation. There are two ways for ISPs to gain market shares: (1) adding higher speed options for their consumers or (2) making use of their service (seem) safer. Without these two benefits no ISP would implement this protocol, due to the negligible possibility of an ROI. A third reason for ISPs to implement DNSSEC is to avoid losing DNS market share to companies who are offering DNS services. While it might seem that this is not an important market share for the ISPs and instead is a cost they would like to avoid, the reality that not providing a DNSSEC service is likely to speed their transition to being simply a bit pipe provider.

5.2.1 Google

Google's new public DNS does not use DNSSEC and instead have implemented a private security system [10]. The purpose of their operating a public DNS service could be to monitor DNS activity and Internet trends among users, enabling improved target marketing. This type of information is worth a lot to Google since it helps improve their click-through rates, which increases their income. There is a great value in knowing what the major Internet sites are. In addition Google can learn demographical information about the users leading to highly valued advertisement information. A major part of Google's revenue is maintained from selling advertisements – but they only make money when someone click on an ad, hence they want to match the ads to the user. This income source accounted for over 98 percent of Google's total revenue (in 2005) of $6.14 billion [16]. It is not only Google that is taking advantage of the opportunity of making income based upon advertising, in fact, quite the opposite. A lot of actors are attempting to generate money through advertisements and the total revenue for search engines that auction advertisements exceeded $150 billion as of May 2006 [16].

However, Google claims that they will implement DNSSEC once their root is signed [17], which is a valid stance since an earlier implementation would not be very beneficial. They support EDNS0 extensions and are thus capable of accepting and forwarding DNSSEC messages, but are not yet validating them. This underlines the importance of deployment in the top levels of the hierarchy as Islands of security without a signed root will not fulfill their full potential until their chain of trust reaches all the way to the root.

5.2.2 TeliaSonera

TeliaSonera is one of Sweden's largest IPSs and owns most of the fixed telephone lines, through which many Internet users are connected (even customers to other ISPs). For TeliaSonera's implementation of DNSSEC the high complexities, foremost with DNSSEC hosting, is the biggest problem [14]. Due to this increased complexity a high cost for implementation is unavoidable. Due to their ongoing expansion TeliaSonera has not made an ROI calculation, which in our opinion is quite risky. They have at least identified the risk related to resolver adoption, which indicates they have done some risk analysis. They realized that DNSSEC could be a waste of resources if the DNS resolvers do not adopt DNSSEC [10]. As most users use the resolvers of their domestic ISPs, this is something they cannot control. Their goals at the moment are to maintain (and promote) their brand, provide secure and solid solutions, and create additional value in other businesses.

At the moment DNSSEC is not marketed by TeliaSonera, primarily because DNSSEC hosting is not yet implemented, this will be needed to provide added security value to their customers [14]. This could also be an indication that DNSSEC is going to be a hygiene factor for ISPs in the future [18]. Hygiene factors are, simply put, something that is expected by the customers and as such it will not give a competitive advantage. However, as customers expect the factor to be provided, an ISP that does not fulfill these demands will be considered a poor choice and will lose market shares. However, TeliaSonera is not famous for marketing their strengths well and it could be a case of them being unable to see a marketing opportunity. Since DNSSEC is a protocol that easily can be implemented to new routers, implementing it will not increase the economical entry barrier for new competitors [19]. While the knowledge barrier increases quite a bit for companies and their employees, and also leads to a cost increase for companies in terms of the cost of supplementary training. A positive consequence of this could be more fulfilled employees due to the sense of achievement which is placed high in Maslow's hierarchy of needs [20].

5.3 Private consumers

The biggest incentive for a private consumer to use DNSSEC is the possibility of being able to trust that the recipient is the intended one. A major fraction of Internet users are concerned with the sensitive information they transmit, whether it is credit card numbers, photos, or other personal information. An implementation of DNSSEC could give a greater sense of security knowing that the information received is correct and has not been altered. However, people will never be able to feel fully secure, due to the simple fact that the Internet never will have perfect security.

Depending on the political scene there is a possibility that consumers may disagree about whether speed or security is the most important attribute of the Internet. But at present when the maximum bandwidth has increased at a rapid pace there could be an opening for an increase in security even though it might increase latency. As long as this extra security does not take more than the extra bandwidth that has been available consumers should not experience a slower end product.

We expect that consumers will require security from their ISPs, but these consumers are in general not likely aware of the different systems and threats. Therefore, these consumers are likely to be content as long as some kind of security system is in place and they would not appreciate any decreases in bandwidth or performance. The consumers also do not want to have security problems – hence most are happy to pay someone else to avoid problems.

The performance demands of the public could also give an incentive to implement improved solutions such as SK-DNSSEC. Customers always demand higher performance and may not be willing to take a step backward due to things that are being promoted as "new improvements".

6. Conclusions

The rate of DNSSEC deployment has increased in the last few years, but there is still a long way to go before global implementation is achieved and DNS attacks are a thing of the past.

Currently a commercial organization has little or no incentive to implement DNSSEC if it only connects them to an island of security without a chain of trust to the root, as highlighted by Google's reluctance to implement DNSSEC into their new DNS service. Once the deployment at the root is completed the deployment in the TLDs should be the highest priority, as it could potentially create a floodgate scenario where the deployment rate rises significantly once the root DNS servers are all using DNSSEC. However, implementing DNSSEC at the TLD level is not enough. Even in Sweden where DNSSEC has been in active use since 2007 commercial organizations are still skeptical about the benefits. The potential security benefits do not seem to be sufficient incentive enough on their own, there must be some apparent potential for increased (or maintaining) market share. Without an expansion of market share there is no ROI which is the primary goal for companies when they choose what investment to make. A project with negative ROI is by definition a failure and a project must either show potential for very high ROI or have a very high likelihood of positive ROI to be interesting. An alternative reason for some companies to implement DNSSEC will be because it mitigates a large risk – since if DNSSEC is available and sufficiently widely used, then failure to utilize it leading to a large loss could mean that the corporate officers have breached their fiduciary duty to their shareholders.

One problem is marketability, while the general public might be aware of security threats they are seldom aware of the nature of these threats. As long as there is some security system in place they assume that they are protected. DNSSEC is by its nature not very attractive: while it offers unique protection it comes with the ball and chain of increased latency. This added latency has proved to be quite miniscule and there is even potential to increase DNS performance through the chain of trust. Since the chain of trust allows you to trust the closest resolver explicitly DNS queries does not have to travel through the hierarchy.

SK-DNSSEC is an interesting proposal that could give the security with an even faster DNS resolution, making it more marketable. However, there are concerns that PK-DNSSEC is not mature enough, and the same concerns will arise with SK-DNSSEC to an even greater extent. PK-DNSSEC has been implemented for a while and most of the inherent and early problems

have been ironed out. With wider deployment problems might surface, but they will need to be corrected quickly (similar to beta testing). This makes a move to SK-DNSSEC risky as the process may have to be repeated with fiascos similar to the one for PK-DNSSEC in Sweden. In the end a seamless implementation could allow for an eventual move to SK-DNSSEC, provided that there is a careful deployment plan.

Letting the invisible hand of the free market [21] control the deployment will likely result in a long process and management control measures from governments should perhaps be used to speed up the process. This will lower the bar for positive ROI and make the project more attractive. Another way could be to make a big deal publically of the deployment of DNSSEC for your TLD. This would make the consumers aware of DNSSEC and create pressure on other corporations to implement it. The downturn of the economy also factors in, as investors tend to be more frugal in uncertain times. However, the deployment rate increased significantly during 2008, thus one might expect that the deployment rate could be even higher as the economy recovers [9].

7. Future research

This thesis provides a good basis for a further study of DNSSEC implementation and it impact(s). A possible investigation is to look beneath the TLDs and see if a corporation that could get the full effect of DNSSEC has not yet implemented it. For example, it would be interesting to see what one specific company can gain from adding DNSSEC to their system. This research should generate additional quantitative data, both in terms of financial benefit and improved customer relations.

Another interesting study would be to compare companies which compete within the same market, to see what benefits they may each get depending on how early they implement DNSSEC. The expected result from such a study should be an estimate of the optimal stage for implementing DNSSEC. Two components would be interesting to compare in a graph, market growth and DNSSEC benefits in security. A comparison between these two variables could show the perfect time for a company to implement DNSSEC. This knowledge could be very useful in the future when implementing other similar upgrades. Hence the market benefits (shown as the solid line in Figure 7) are high at first and rapidly decreases depending on how many others have already implemented this solution. While security benefits (shown as a dotted line in Figure 7) are low at first and then rapidly increase depending on how many others have implemented DNSSEC. Combining these two graphics it is easy to see at what time the lines cross each other, as this would be the optimal time for implementing DNSSEC (this point is shown by the arrow in Figure 7). A high gain in both areas is achieved without having the high risk of an early adopter.

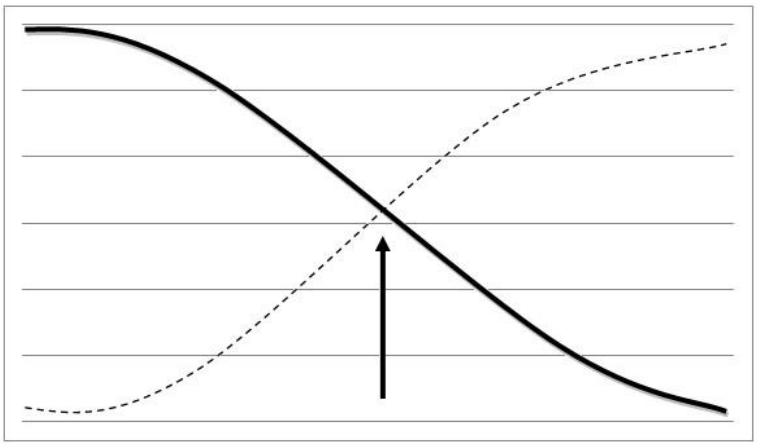


Figure 7 - Optimal implementation time for DNSSEC

References

[1] Donald E. Eastlake 3rd, “Domain Name System Security Extensions”, IETF Network Working Group, Request for comments 2535, March 1999
http://www.rfc-editor.org/rfc/rfc2535.txt

Replaced by:
Roy Arends et al., “DNS Security Introduction and Requirements”, IETF Network Working Group, Request for comments 4033, March 2005
http://www.rfc-editor.org/rfc/rfc4033.txt

Roy Arends et al., “Resource Records for the DNS Security Extensions”, IETF Network Working Group, Request for comments 4034, March 2005
http://www.rfc-editor.org/rfc/rfc4034.txt

Roy Arends et al., “Protocol Modifications for the DNS Security Extensions”, IETF Network Working Group, Request for comments 4035, March 2005
http://www.rfc-editor.org/rfc/rfc4035.txt

[2] Giuseppe Ateniese and Stefan Mangard, “A new approach to DNS security (DNSSEC)”,
In the Proceedings of the 8th ACM conference on Computer and Communications Security (CCS '01), ACM, New York, NY, USA, ISBN: 1-58113-385-5, November 2001, pages 86-95, http://doi.acm.org/10.1145/501983.501996;
also available from: http://www.cs.jhu.edu/~ateniese/papers/dnssec.pdf

[3] Eric Osterweil, Dan Massey, and Lixia Zhang,
"Managing Trusted Keys in Internet-Scale Systems",
In Proceedings of the 2009 Ninth Annual International Symposium on Applications and the Internet (SAINT '09), IEEE Computer Society, Washington, DC, USA, ISBN: 978-0-7695-3700-9,July 2009, pages 153-156,
http://dx.doi.org/10.1109/SAINT.2009.38
also available from: http://www.cs.ucla.edu/~eoster/doc/tas-fist09.pdf

[4] Stefan Roelofs, “Ad-hoc Trust Associations with Trust Anchor Repositories”, Technical report, System and Network Engineering (SNE), Universiteit van Amsterdam, 2 July 2009; available from:
http://www.delaat.net/~cees/sne-2008-2009/p16/report.pdf

[5] Paul Wouters, "DNSSEC: Theory and Worldwide Operational Experiences",
Presentation at SecTor (Security and Education Conference), October 25-27, 2010, Toronto, ON, Canada; available from:
http://www.xelerance.com/talks/sector/Sector2007DNSSEC.pdf

[6] Lauren Price, "Another Attack, Another Reason for the Urgency of DNSSEC Adoption",
Blog entry, CircleID. Iomemo Inc., May 01, 2009 10:58 AM PDT; available from:
http://www.circleid.com/posts/20090501_another_attack_another_reason_for_dnssec/

[7] Internet World Stats, Top 20 countries with highest number of Internet users, Miniwatts Marketing Group, 19 November 2009; available from:
http://www.internetworldstats.com/top20.htm

[8] Organization for Economic Co-operation and Development (OECD), Website, http://www.oecd.org/, last modified 27 May 2010.

[9] Eric Osterweil, Dan Massey, and Lixia Zhang, "Deploying and Monitoring DNS Security (DNSSEC)," In the proceedings of the 2009 Annual Computer Security Applications Conference (ACSAC 2009), IEEE Computer Society, Los Alamitos, CA, USA, ISSN 1063-9527, 2009, pp.429-438 http://doi.ieeecomputersociety.org/10.1109/ACSAC.2009.47

[10] Electronic Privacy Information Center (EPIC), "Google Expands Control of Internet Architecture", News item, EPIC, Dec. 8, 2009; available from: http://epic.org/privacy/dnssec/

[11] Jacob Schlyter, "DNSSEC Validation Performance Testing", Presentation at IETF '65, March 19-24, 2006, Dallas, TX, USA; available from: http://www.ietf.org/proceedings/65/slides/dnsop-0.pdf

[12] Thierry Moreau, "DNSSEC is almost worthless!", E-mail posting to namedroppers@ops.ietf.org, Sunday 5 Mar 2006 11:58:17 -0500; available from: http://www.ops.ietf.org/lists/namedroppers/namedroppers.2006/msg00241.html

[13] "DNSSEC – The path to a secure domain", Web page, .SE - The Internet Infrastructure Foundation, last modified 2010.05.27; available from http://www.iis.se/en/domaner/dnssec

[14] Interview with Hans Åkesson (Safety Manager) and Mats Dufberg (DNSSEC expert), TeliaSonera, Stockholm, Sweden, interviewed on 2010.05.12

[15] J. Abley, D. Knight, and M. Larson, "DNSSEC Deployment for the Root Zone" Draft techinical report, Internet Corporation For Assigned Names and Numbers (ICANN), Root DNSSEC Design Team, May 5, 2010; available from http://www.root-dnssec.org/wp-content/uploads/2010/05/draft-icann-dnssec-deployment-02.txt

[16] Benjamin Edelman, Michael Ostrovsky and Michael Schwartz, "Internet Advertising and the Generalized Second Price Auction: Selling Billions of Dollars Worth of Keywords", American Economic Review, v. 97(1), March 2007, pp. 242-259; available from: http://faculty-gsb.stanford.edu/ostrovsky/papers/gsp.pdf

[17] Patrik Wallström, "Google Public DNS", web page,Internetdagarna, .SE - Stiftelsen för Internetstruktur, 2009.12.07, available from: http://www.internetdagarna.se/track/ip-och-infrastruktur/google-public-dns

[18] Frederick Herzberg, "One More Time: How Do You Motivate Employees?" Harvard Business Review, Harvard Business Press, May 14, 2008 80 pages, ISBN-10: 1422125998, ISBN-13: 978-1422125991; available from: http://www.facilitif.eu/user_files/file/herzburg_article.pdf

[19] Michael E. Porter, "How Competitive Forces Shape Strategy", Harvard Business Review, March/April 1979; available from: http://www.business.umt.edu/faculty/Wishcamper/Entrepreneurship/Competitive%20Forces.pdf

[20] Abraham Harold Maslow, “Motivation and Personality”,
HarperCollins Publishers; 3 Sub edition, January 1987
293 pages, ISBN-10: 0060419873, ISBN-13: 978-0060419875
(originally published in 1954)

[21] Adam Smith, “The Theory of Moral Sentiments”, Penguin Classics, Anniversary edition, January 26, 2010 (originally published in 1759),
528 pages, ISBN-10: 0143105922, ISBN-13: 978-0143105923

Appendix A – SecSpider Research Data

Table 1 – Top 20 ccTLDs

DNSSEC deployment in TLDs of the Top 20 countries in Internet usage [7].

Top 20 ccTLDs	EDNS0	DNSSEC	# of Users	% of Usage
.br	Yes	Yes	67510400	3,89%
.ca	Yes	No	25086000	1,45%
.cn	Yes	No	360000000	20,76%
.de	Yes	No	61973100	3,57%
.es	Yes	No	29093984	1,68%
.fr	Yes	No	43100134	2,49%
.id	Yes	No	30000000	1,73%
.in	Yes	No	81000000	4,67%
.ir	Yes	No	32200000	1,86%
.it	Yes	No	30026400	1,73%
.jp	Yes	No	95979000	5,54%
.kr	Yes	No	37475800	2,16%
.mx	Yes	No	27600000	1,59%
.ph	Yes	No	24000000	1,38%
.pl	Yes	No	20020362	1,15%
.ru	Yes	No	45250000	2,61%
.tr	Yes	No	26500000	1,53%
.uk	Yes	Yes	46683900	2,69%
.us	Yes	Yes	234372000	13,52%
.vn	Yes	No	21963117	1,27%
Total			1339834197	77,27%
World users:			1733993741	100,00%

Table 2 – gTLDs

DNSSEC deployment in the gTLDs [7].

gTLDs	EDNS0	DNSSEC
.aero	Yes	No
.asia	Yes	No
.biz	Yes	No
.cat	Yes	No
.com	Yes	No
.coop	Yes	No
.edu	Yes	No
.gov	Yes	Yes
.info	Yes	No
.int	Yes	No
.jobs	Yes	No
.mil	Yes	No
.mobi	Yes	No
.museum	Yes	Yes
.name	Yes	No
.net	Yes	No
.org	Yes	Yes
.pro	Yes	No
.tel	Yes	No
.travel	Yes	No

Table 3 – OECD ccTLDs

DNSSEC deployment in TLDs of the OECD countries [7].

OECD ccTLDs	EDNS0	DNSSEC	# of Users	% of Usage
.au	Yes	No	17033826	0,98%
.be	Yes	No	7292300	0,42%
.ch	Yes	Yes	5739300	0,33%
.cl	Yes	No	8369036	0,48%
.cz	Yes	Yes	6027700	0,35%
.de	Yes	No	61973100	3,57%
.dk	Yes	No	4629600	0,27%
.es	Yes	No	29093984	1,68%
.fi	Yes	No	4382700	0,25%
.fr	Yes	No	43100134	2,49%
.gr	Yes	No	4932495	0,28%
.hu	Yes	No	5873100	0,34%
.ie	Yes	No	2830100	0,16%
.is	Yes	No	285700	0,02%
.it	Yes	No	30026400	1,73%
.jp	Yes	No	95979000	5,54%
.kr	Yes	No	37475800	2,16%
.lu	Yes	No	387000	0,02%
.nl	Yes	No	14304600	0,82%
.no	Yes	No	4235800	0,24%
.nz	Yes	No	3500000	0,20%
.pl	Yes	No	20020362	1,15%
.se	Yes	Yes	8085500	0,47%
.uk	Yes	Yes	46683900	2,69%
.us	Yes	Yes	234372000	13,52%
Total			696633437	40,18%
World users:			1733993741	100,00%

Table 4 – DNSSEC ccTLDs

All ccTLDs within our restriction with DNSSEC fully deployed [7].

DNSSEC ccTLDs	EDNS0	DNSSEC	# of Users	% of Usage
.ch	Yes	Yes	5739300	0,33%
.cz	Yes	Yes	6027700	0,35%
.se	Yes	Yes	8085500	0,47%
.uk	Yes	Yes	46683900	2,69%
.us	Yes	Yes	234372000	13,52%
.br	Yes	Yes	67510400	3,89%
Total			368418800	21,25%
World users:			1733993741	100,00%

Appendix B – DNS Benchmarking

Table 5 – Without Authentication Averages

The average data of the research made without DNSSEC authentication.

Server IP	Cached Min	Cached Avg	Cached Max	Cached Std	Uncached Min	Uncached Avg	Uncached Max	Uncached Std	Dotcom Min	Dotcom Avg	Dotcom Max	Dotcom Std
10. 0. 1. 1	0,001	0,001	0,0035	0,001	0,0295	0,1175	0,329	0,094	0,0095	0,047	0,281	0,0615
8. 8. 8. 8	0,0255	0,03	0,0415	0,0035	0,0425	0,1555	0,4145	0,104	0,046	0,088	0,1895	0,0395
8. 8. 4. 4	0,0245	0,03	0,044	0,004	0,044	0,1565	0,398	0,104	0,0465	0,075	0,1555	0,0255
204. 117. 214. 10	0,027	0,0315	0,04	0,0025	0,03	0,1105	0,437	0,102	0,037	0,044	0,0545	0,0035
199. 2. 252. 10	0,028	0,032	0,0395	0,0025	0,0305	0,1065	0,407	0,0955	0,037	0,0455	0,056	0,0045
204. 97. 212. 10	0,0285	0,033	0,0395	0,0025	0,0305	0,109	0,4295	0,1015	0,0385	0,0455	0,057	0,0045
129. 250. 35. 251	0,031	0,035	0,0455	0,0025	0,034	0,1125	0,383	0,0935	0,039	0,073	0,241	0,049
129. 250. 35. 250	0,031	0,035	0,0425	0,002	0,0335	0,115	0,396	0,098	0,0395	0,0665	0,181	0,0415
156. 154. 71. 1	0,031	0,0355	0,0435	0,0025	0,035	0,1265	0,3595	0,101	0,0335	0,0415	0,051	0,004
4. 2. 2. 3	0,031	0,037	0,0465	0,0035	0,0345	0,1315	0,5495	0,111	0,034	0,102	0,2915	0,0695
208. 67. 220. 220	0,033	0,0375	0,054	0,004	0,036	0,223	1,3115	0,297	0,039	0,1295	0,3445	0,0745

Table 6 – With Authentication Averages

The average data of the research made with DNSSEC authentication.

Server IP	Cached Min	Cached Avg	Cached Max	Cached Std	Uncached Min	Uncached Avg	Uncached Max	Uncached Std	Dotcom Min	Dotcom Avg	Dotcom Max	Dotcom Std
10. 0. 1. 1	0,001	0,002	0,0075	0,001	0,0295	0,1155	0,323	0,09	0,009	0,064	0,3335	0,093
199. 2. 252. 10	0,027	0,0315	0,039	0,0025	0,032	0,1095	0,445	0,1025	0,036	0,0455	0,058	0,0055
204. 97. 212. 10	0,027	0,0315	0,0395	0,0025	0,03	0,1145	0,4715	0,115	0,0365	0,044	0,054	0,0045
8. 8. 8. 8	0,0245	0,0305	0,038	0,003	0,042	0,149	0,4175	0,1045	0,0465	0,0795	0,166	0,03
8. 8. 4. 4	0,025	0,0305	0,0395	0,003	0,044	0,1575	0,4225	0,1085	0,045	0,094	0,205	0,045
204. 117. 214. 10	0,0285	0,034	0,0425	0,003	0,033	0,113	0,4465	0,1085	0,0385	0,047	0,058	0,0045
129. 250. 35. 251	0,031	0,035	0,0435	0,003	0,034	0,1135	0,393	0,096	0,0395	0,0895	0,315	0,0795
129. 250. 35. 250	0,032	0,0365	0,045	0,0025	0,0345	0,113	0,394	0,095	0,0415	0,078	0,312	0,0665
156. 154. 71. 1	0,031	0,036	0,0425	0,002	0,034	0,1225	0,371	0,1035	0,0345	0,0435	0,0535	0,005
4. 2. 2. 3	0,0335	0,038	0,0465	0,0025	0,038	0,147	0,574	0,1275	0,037	0,0875	0,291	0,0525
156. 154. 70. 1	0,034	0,039	0,047	0,003	0,0385	0,1205	0,364	0,094	0,037	0,0445	0,054	0,003

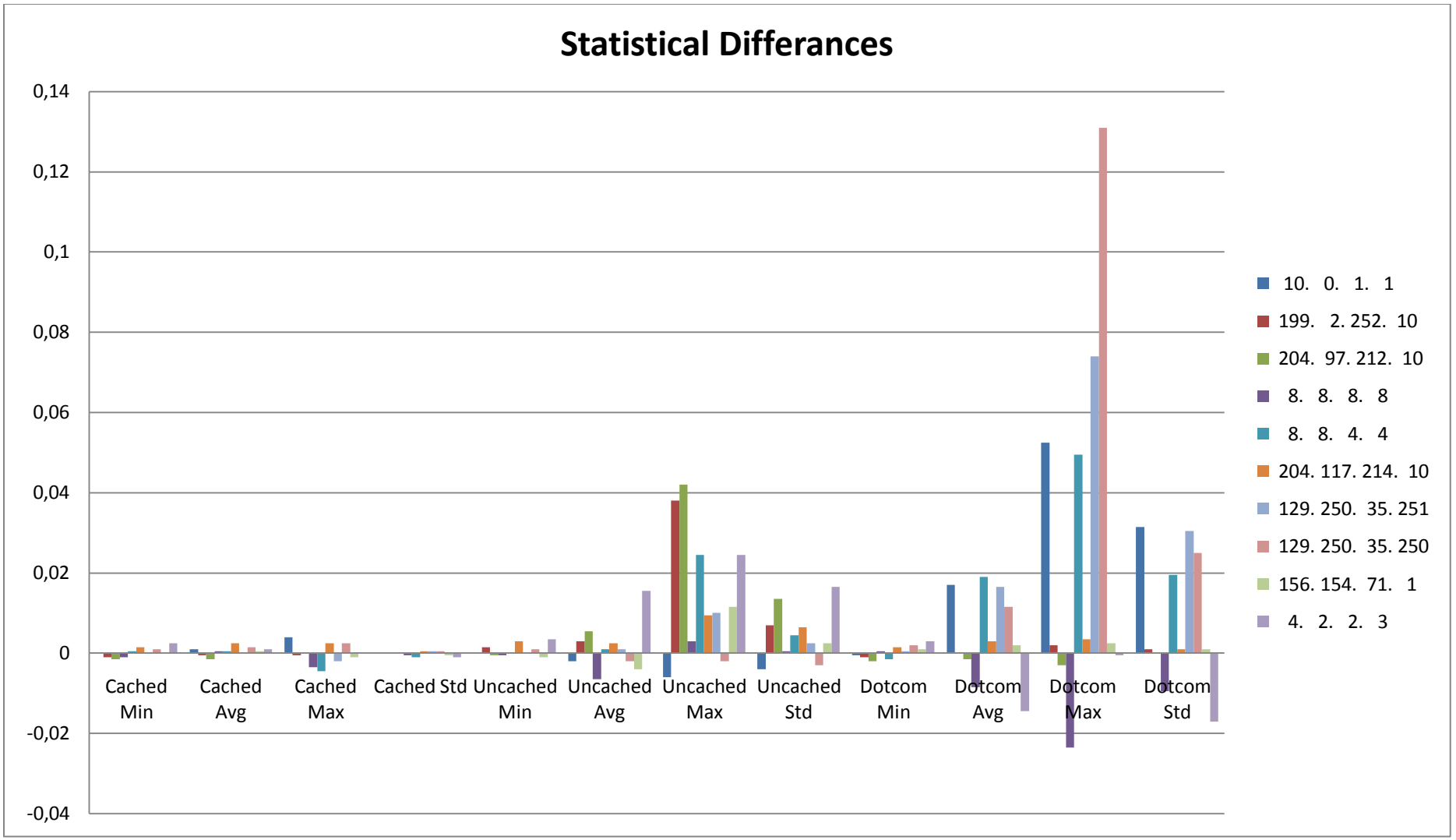
Table 7 – Differences

The differences between the averages – a positive number indicates that traffic was slower with DNSSEC authentication.

Server IP	Cached Min	Cached Avg	Cached Max	Cached Std	Uncached Min	Uncached Avg	Uncached Max	Uncached Std	Dotcom Min	Dotcom Avg	Dotcom Max	Dotcom Std
10. 0. 1. 1	0	0,001	0,004	0	0	-0,002	-0,006	-0,004	-0,0005	0,017	0,0525	0,0315
199. 2. 252. 10	-0,001	-0,0005	-0,0005	0	0,0015	0,003	0,038	0,007	-0,001	0	0,002	0,001
204. 97. 212. 10	-0,0015	-0,0015	0	0	-0,0005	0,0055	0,042	0,0135	-0,002	-0,0015	-0,003	0
8. 8. 8. 8	-0,001	0,0005	-0,0035	-0,0005	-0,0005	-0,0065	0,003	0,0005	0,0005	-0,0085	-0,0235	-0,0095
8. 8. 4. 4	0,0005	0,0005	-0,0045	-0,001	0	0,001	0,0245	0,0045	-0,0015	0,019	0,0495	0,0195
204. 117. 214. 10	0,0015	0,0025	0,0025	0,0005	0,003	0,0025	0,0095	0,0065	0,0015	0,003	0,0035	0,001
129. 250. 35. 251	0	0	-0,002	0,0005	0	0,001	0,01	0,0025	0,0005	0,0165	0,074	0,0305
129. 250. 35. 250	0,001	0,0015	0,0025	0,0005	0,001	-0,002	-0,002	-0,003	0,002	0,0115	0,131	0,025
156. 154. 71. 1	0	0,0005	-0,001	-0,0005	-0,001	-0,004	0,0115	0,0025	0,001	0,002	0,0025	0,001
4. 2. 2. 3	0,0025	0,001	0	-0,001	0,0035	0,0155	0,0245	0,0165	0,003	-0,0145	-0,0005	-0,017

Charts

The data from Table 7 put into a chart for visual interpretation.



TRITA-ICT-EX-2010:108

www.kth.se