



**DNSSEC:**

EVERYTHING YOU WANTED TO KNOW AND  
MORE

1775 Wiehle Ave • Suite 200 • Reston, VA 20190 USA • 703.889-5778 • [www.pir.org](http://www.pir.org)



## **Introduction**

Today more than ever, there is greater scrutiny on online security. As internet attacks increase, it is more important than ever to secure the Domain Name System (DNS) in order to handle the highly sophisticated threats that exist on the internet today. The bad guys are getting smarter and the attacks they are carrying out are too complex for our current Domain Name System (DNS) to handle.

But there is hope. We can secure The Domain Name System (DNS) through a security measure called DNS Security Extensions (DNSSEC).

Use this guide as an introduction to the Domain Name System structure and the implementation of the security measure called DNSSEC.

## **The Domain Name System (DNS)**

The Domain Name System (DNS) is one of the key components to the Internet. The Domain Name System (DNS) has a very important job and that is to locate and translate domain names into Internet Protocol or IP addresses. For example, [www.123.org](http://www.123.org) would translate into 106.67.543.568.

*Why is this important?*

A domain name has meaning to internet users and domain names are easy for the users to remember.

## **What is DNSSEC**

DNS Security Extensions (DNSSEC) adds security to the Domain Name System.

It is a set of extensions to DNS, which provide:

1. Origin Authentication of DNS Data
2. Data Integrity
3. Authenticated Denial of Existence.

## **How does DNSSEC it work?**

DNS Security Extensions (DNSSEC) uses cryptographic electronic signatures signed with a trusted digital certificate to determine the authenticity of data.

## **What kind of attacks does DNSSEC protect users from?**

DNS Security Extensions (DNSSEC) was designed to protect the Internet from certain attacks, such as DNS cache poisoning and Doman Hijacking also known as Man in the Middle Attacks.

## Cache Poisoning, Domain Hijacking, Bad Guys in the Middle? What do you mean?

Here is an example that is simple to understand.

Today, you pick up a telephone and you dial a series of numbers in order to reach the person you want to speak to. If you know you dialed the numbers correctly, you can be assured that the person on the other line is the person you intended to speak with. Well, the current Domain Naming System is designed in such a way that this assurance is not possible. So if a user types in a web address, it is possible that a "bad guy" can interrupt that transaction and take the user to a phony website without the user even knowing this occurred. Imagine if the end user proceeded to enter in highly sensitive information like their bank account number. Imagine how catastrophic this would be to the online reputation of the website owner.



### How real are these types of attacks?

*In March-April 2005*, users of an ISP had specific spyware, spam and pay-per-click trojans, from redirection sites

The ISP's cache had hundreds of DNS names spoofed...

- AmericanExpress.com
- FedEx.com
- CitiCards.com
- DHL-USA.com
- Sabre.com

Source: Allison Mankin <http://www.psg.com/~mankin/vita.txt>

*In April of 2009*, a Domain Name System cache poisoning attack was carried out on a prominent financial institution's website in Brazil. Users were redirected to a phony server where the attackers were in a position to steal the bank users' passwords.

Source: [http://www.thewhir.com/web-hosting-news/042309\\_DNS\\_Cache\\_Poisoning\\_Targets\\_Brazilian\\_Bank](http://www.thewhir.com/web-hosting-news/042309_DNS_Cache_Poisoning_Targets_Brazilian_Bank)

### What kind of .ORG customers should use DNS Security Extensions (DNSSEC)

Everyone but most importantly, large financial institutions such as credit unions, associations or nonprofit organizations that have online donations coming through their website, a large domain name portfolio holder who wants to ensure traffic goes to their website or any other .ORG domain holder that has highly sensitive data transactions occurring on their websites.



### **Protect yourself today**

Just imagine how disastrous it would be if you or your organization became the victim of a cache poisoning or domain hijack attack? Protect your hard earned online reputation today with DNSSEC.

### **Resources & Further Reading**

For further information on DNSSEC and its implementation throughout the Internet, please visit the sites below:

#### **DNSSEC Industry Coalition** (<http://dnsseccoalition.org>)

The DNSSEC Industry Coalition is a global group of registries and industry experts whose mission is to work collaboratively to facilitate adoption of Domain Name Security Extensions (DNSSEC) and streamline the implementations across Domain Name Registries. The coalition was founded in August 2008 by .ORG, The Public Interest Registry.

#### **Secure64** (<http://www.secure64.com/how-to-dnssec-information>)

Secure64 is a software company offering high-performance DNS server software that makes the DNS trustworthy and secure.

#### **DNSSEC-Deployment** (<http://dnssec-deployment.org/>)

The DNSSEC Deployment Working Group is a group of experts active in the development or deployment of DNSSEC. It is open for anyone interested in participation.

#### **DNSSEC-Tools** (<http://dnssec-tools.org/>)

The goal of the DNSSEC-Tools project is to create a set of software tools, patches, applications, wrappers, extensions, and plugins that will help ease the deployment of DNSSEC related technologies.

#### **DNSSEC.net** (<http://dnssec.net/>)

The DNSSEC.net website is your independent starting point for all DNSSEC related information. It contains references to all major DNSSEC projects, presentations, research work, DNSSEC enabled software, and IETF reference material.

#### **DNSStuff.com** (<http://dnsstuff.com/>)

DNSstuff helps you configure, monitor and fix problems with your domain and email. Our tools and alerts provide insight into your domain from the outside looking in.

#### **InfoBlox** (<http://infoblox.com/>)

Infoblox pioneered the development of core network services appliances, which deliver utility-grade domain name resolution (DNS).

#### **Internet Systems Consortium, Inc. (ISC)** (<http://isc.org/>)

The proud to be the producer and distributor of commercial quality Open Source software for the Internet Community