Summer 2010

Evaluation of Dnssec in Microsoft Windows and Microsoft Windows Server 2008 R2

Christopher Hair
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Abstract

The Domain Name System (DNS) provides important name resolution services on the Internet. The DNS has been found to have security flaws which have the potential to undermine the reliability of many Internet-based systems. DNS Security Extensions (DNSSEC) offers a long-term solution these DNS security flaws. However, DNSSEC adoption has been slow because it is challenging to deploy and administer. DNSSEC has also been criticized for not being an "end-to-end" solution. Microsoft included support for DNSSEC in its latest operating systems, Windows Server 2008 R2 and Windows 7. This thesis concluded that DNSSEC features in Windows Server 2008 R2 and Windows 7 are not fully developed and are unlikely to impact DNSSEC adoption rates.

Table of Contents

List of Figures

List of Tables

Chapter 1 – Introduction

The Domain Name System (DNS) is a foundational service of the Internet, and the DNS is showing cracks in the form of security vulnerabilities. DNS Security Extensions (DNSSEC) provides a layer of security to close those security gaps. However, DNSSEC adoption rates have been low. Microsoft, a major technology vendor, released new operating systems Windows 7 and Windows Server 2008 Release 2 (R2) in late 2009. These new operating systems offer DNSSEC features. This thesis will evaluate whether the latest Microsoft offerings provide significant advancements in DNSSEC technology which could lead to increased adoption of DNSSEC.

The DNS translates user-friendly domain names (e.g. www.regis.edu) into network-friendly IP addresses (e.g. 207.93.211.100). The original designers of DNS did not include security as one of the design goals. Today, it is understood that DNS-related security vulnerabilities exist, and that they have the potential to undermine the reliability of many Internet services (Atkins & Austein, 2004; Chandramouli & Rose, 2006). In light of increased commercial use of the Internet, security vulnerabilities in a fundamental building block of the Internet (DNS) could have wide-ranging detrimental effects on finance, commerce, and the economy (United States, 2003, p. 30).

DNSSEC is a suite of IETF specifications designed to add security to DNS and protect against certain vulnerabilities (Arends, Austein, Larson, Massey & Rose, 2005; Eastlake & Kaufmann, 1997). The current core specifications are IETF RFCs 4033, 4034 and 4035 (Arends et al., 2005). DNSSEC adds a layer of authentication to DNS, so a DNS caching server requesting a DNS lookup from an authoritative DNS server has assurance that the response is correct. DNSSEC does not provide confidentiality—Internet DNS records are intended to be

visible (Arends et al., 2005). DNSSEC does not protect against distributed denial of service (DDoS) attacks. In fact, the increased overhead of DNSSEC could make DNS more vulnerable to DDoS (Arends et al., 2005).

Adoption of DNSSEC has been slow, but interest in DNSSEC has increased significantly since July 2008 when Dan Kaminsky presented a paper describing a relatively easy way to exploit a vulnerability in DNS to carry out DNS cache poisoning attacks (The Internet Infrastructure Foundation, n.d.; Morris, n.d.). Before the "Kaminsky" paper, it was widely believed that DNSSEC was a solution to a largely-theoretical problem. Other problems were more pressing. Kaminsky illustrated a real DNS security problem, and DNSSEC offers the only long-term solution (Friedlander, Mankin, Maughan, & Crocker, 2007; The Internet Infrastructure Foundation, n.d.).

Microsoft Windows Server 2008 R2 and Windows 7, both released in 2009, are the first Microsoft operating systems that support the three core DNSSEC specifications (RFCs 4033, 4034 and 4035) (Microsoft, 2009). Windows 7 is the first client operating system to offer a bundled DNSSEC solution (Microsoft, 2009). Support from Microsoft, a company that controls a large share of the operating system market, is an indication that DNSSEC may become a "mainstream" technology.

This thesis will test and evaluate whether the latest Microsoft operating systems provide solutions to the problems that have resulted in slow DNSSEC adoption. Is DNSSEC easy to deploy in Microsoft Windows Server 2008 R2 and Windows 7? Now that DNSSEC is bundled with a Microsoft client operating system for the first time, can one consider this an "end-to-end" DNSSEC solution for the mass market? Does DNSSEC in Windows 7 provide the end user with

meaningful, actionable feedback? Is Windows DNSSEC compatible with Unix/BIND DNSSEC? Is administration of DNSSEC in windows server 2008R2 user-friendly?

The testing procedures take place in a lab environment with several operating systems installed as virtual machines. The lab includes four virtual machines, described in detail in Appendix A: Two Microsoft Windows Server 2008 R2 with DNS Server and DNSSEC, Windows 7 Professional with the "non-validating security-aware stub resolver", and Solaris 10 with BIND and DNSSEC extensions. The lab environment is described in detail in Appendix A.

This thesis contributes to the existing DNSSEC literature by evaluating a new offering from one of the largest players in the IT industry. If Microsoft DNSSEC is easy to install and administer, and if it effectively brings DNSSEC to the client level with Windows 7, then this will result in larger numbers of people choosing to deploy DNSSEC. Microsoft has a majority share of the client operating system market. An effective DNSSEC solution from Microsoft could strengthen its hold on the market, could likely lead to quicker adoption of DNSSEC by more businesses, and contribute to increased security for the Internet community as a whole.

Chapter 2 – Overview of DNS, DNSSEC, and Windows DNSSEC

DNS is a Critical Service

The Domain Name System (DNS) is fundamental to the functionality of the Internet. The DNS translates user-friendly host names (e.g. www.regis.edu) into network-friendly IP addresses (e.g. 207.93.211.100) (Liu & Albitz, 2006, Ch. 1). The DNS also enables applications like e-mail to identify servers associated with a service (Liu & Albitz, 2006, Ch. 5). Imagine these conversations between people that would be necessary without the DNS: "Please visit my web site at 207.93.211.100." "Send me an e-mail at hair289@207.93.211.120. If 207.93.211.120 fails to respond, please send the message to one of these alternate mail servers in this order of priority: 207.93.211.121, 207.93.211.122, 207.93.211.123, or 207.93.211.124." The Internet would not function as it currently does without the DNS.

The DNS is designed for scalability and availability as a distributed database (Liu & Albitz, 2006, Ch. 2). The namespace structure is a hierarchical tree starting at the root or ".". The first branches are top level domain names (TLDs), then the next level has domain names, as illustrated in Figure 1.

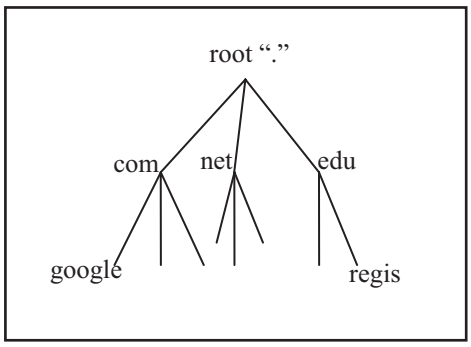

Figure 1. Illustration of the DNS namespace hierarchy.

Each branch in the namespace has one or more authoritative name servers that store information for that domain. The root name servers are authoritative for the root, and store

delegations for name servers that are authoritative for the TLDs. The .edu TLD servers store delegations for name servers that are authoritative for each domain name registered within the .edu TLD, for example, regis.edu. The regis.edu name servers store the hostnames and IP addresses for the regis.edu zone. The delegation of the namespace tree continues as far as needed (Liu & Albitz, 2006, Ch. 2).

The DNS is further distributed by function: DNS servers can perform one or all of these functions: authoritative (primary or secondary), forwarding, resolving, or caching. An authoritative name server stores the zone file containing hostnames and IP addresses for the domain name for which it is authoritative. A resolving name server listens for queries from clients and attempts to resolve the queries through forwarding, recursion, or its own cache. A forwarding name server acts as an intermediary, forwarding queries to Internet name servers. A caching name server stores hostnames and IP addresses which it has already resolved so that it does not have to spend resources (bandwidth, processor) in looking them up again within their TTL (time to live) period (see Figure 2) (Liu & Albitz, 2006, Ch. 2).

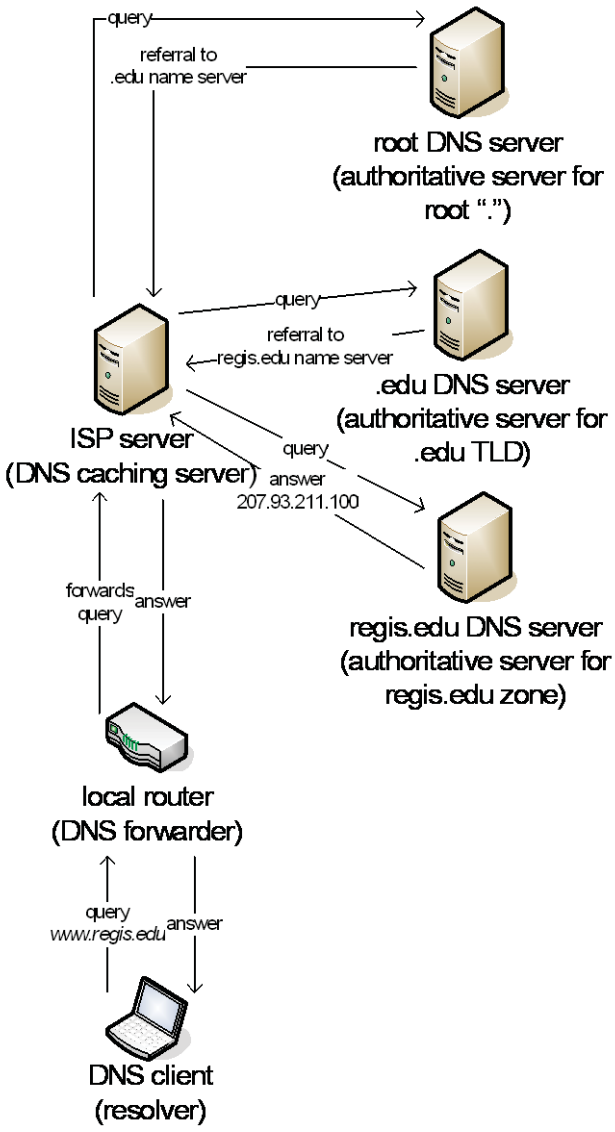

Figure 2. Illustration of DNS server functions.

It is also possible to have private DNS namespaces. Companies commonly maintain DNS namespaces within their private networks, where each server, workstation and device on the private network has a hostname and entry in the private DNS zone file maintained on the internal network name servers. The subject of this paper is the public Internet DNS.

To give an idea of the size and scope of the public Internet DNS: A survey completed in January 2010 found 86,521,299 domain names and 106,044 DNS servers on the Internet (Internet Software Consortium, 2010).

A DNS Query

These are the steps that occur in a typical DNS query for a Windows client that attempts to visit the web site www.regis.edu using a web browser (see Figure 2). The Windows client first checks its local resources (local cache, local hosts file) to determine if it already knows the IP address for www.regis.edu. If not, it issues a DNS query to the IP address configured in its TCP/IP configuration as its DNS server. The resolving/caching DNS server is typically a service provided by the local Information Technology department or the Internet Service Provider. The resolving/caching DNS server checks to see if it is authoritative for the regis.edu zone. If not, it checks its local cache to see if it already knows the answer to the query. If not, it either forwards the query to another DNS server or it uses *recursion* to look up the answer (Davies, 2006). Meanwhile, the Windows client is waiting for a response.

A DNS server that is configured to use recursion has a list of "root hints", which is a list of IP addresses of name servers for the DNS root ".". The name server randomly chooses a root server from its list and queries the root server if it knows the IP address for www.regis.edu. The root server checks its cache and whether it is authoritative for regis.edu. The answer is no. However, the root server has delegations for the TLDs including .edu. The root server responds with a referral to a name server for the .edu TLD. The resolving/caching name server receives the referral and then queries the .edu TLD name server if it knows the IP address for www.regis.edu. The .edu TLD server checks its cache for the answer and whether it is authoritative for regis.edu. The answer is no. However, the .edu server has delegations for all .edu domains including regis.edu. The .edu server responds with a referral to the authoritative name server for regis.edu. The resolving/caching name server receives the referral and then queries the authoritative name server for regis.edu if it knows the IP address for www.regis.edu.

The regis.edu name server knows the answer. It responds that www.regis.edu is 207.93.211.100. The resolving/caching name server adds the answer to its local cache and forwards the answer to the Windows client (Liu & Albitz, 2006, pp. 27-30). The Windows client adds the answer to its local cache, gives the answer to the web browser, and the web browser uses this information to successfully navigate to the web site. All of these steps occur within milliseconds (Davies, 2006).

DNS records have a "time to live" (TTL). The TTL determines how long the record should remain the in the cache of a client or caching name server. The administrator for the authoritative name server for regis.edu configures TTL for www.regis.edu. In Windows, the command to view the local DNS cache is "ipconfig /displaydns". Figure 3 shows the results including how many seconds the record has remaining in the local cache (approximately 10 hours).

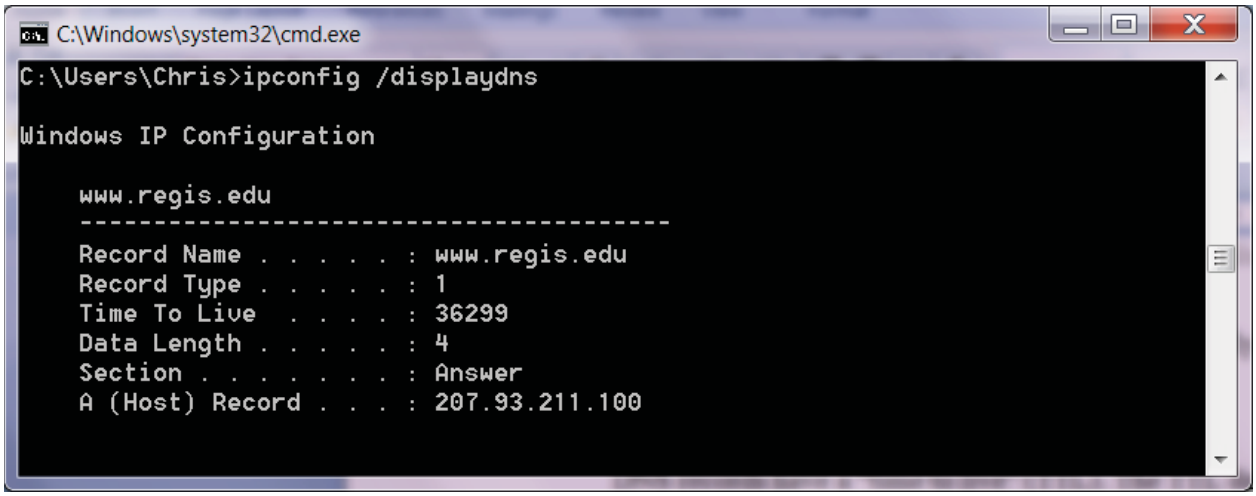

Figure 3. TTL for www.regis.edu.

The next time this Windows client attempts to visit www.regis.edu, as long as it is within the TTL period, it will have the IP address for the web site in its local cache and it will not need to issue a DNS query (Davies, 2006). If a different Windows client queries the caching name server for www.regis.edu within the TTL period, the caching name server will respond with the

answer from its cache and it will not use recursion to find the answer. If the administrator for regis.edu changes the IP address for www.regis.edu it will take time for the change to propagate around the Internet, because any client or server with the old IP address in its cache will wait for the TTL on the old record to expire before it discovers the new record (Liu & Albitz, 2006, pp. 34-36).

DNS Security Vulnerabilities

The DNS is vulnerable to attack by malicious persons in several ways. Hacking and cracking on the Internet is no longer simply the work of vandals or pranksters. Malicious persons are motivated by greed and profit to take advantage of security vulnerabilities. Money in bank accounts, available through fraudulent web-based transactions, is a prime target. The DNS may be attacked at the authoritative servers, caching servers, or the network communication links. IETF RFC 3833 (Atkins & Austein, 2004) outlines a catalog of threats to the DNS.

The "Kaminsky" vulnerability – cache poisoning.

In July 2008, security researcher Dan Kaminsky publicly reported on a vulnerability that was present in all major DNS server software. The vulnerability is due in part to the DNS server software simply following the DNS specifications. The Kaminsky vulnerability is in caching resolvers—the DNS servers at Internet Service Providers that resolve recursive DNS queries on behalf of clients and then "remember" the answers in the cache for a period of time (the TTL). The attacker uses this vulnerability to "poison" the cache with invalid data. Clients of a DNS server with a poisoned cache will be redirected to the attacker's web site. The attack can be used as part of a phishing scheme (The Internet Infrastructure Foundation, n.d.).

A caching DNS server that does not already have the answer to a query in its cache uses recursion to resolve the query. The goal of an attacker is to interfere with the communication

between the resolver and the DNS servers it is querying, providing invalid information before the response comes back from the valid DNS server. If the attacker is successful, when the valid response comes back the caching resolver will drop the valid response as a duplicate (The Internet Infrastructure Foundation, n.d.).

When DNS servers communicate with each other, they use a 16-bit transaction ID to validate the response they receive back. A 16-bit transaction ID means the transaction ID can be between 1 and 65,536 (base 10). Thus, an attacker sending spoofed responses to a caching resolver has about a 1 in 65,000 chance of guessing the correct transaction ID. Kaminsky also observed that the transaction ID used by some DNS servers is less than random. Some DNS servers use sequential transaction IDs, making it easy to guess the next one. An attacker can automate the process of issuing cache poisoning attempts, and with enough time can successfully guess a valid transaction ID and poison a DNS server's cache. With current computing power (an attacker controlling a single computer), a successful attack on a vulnerable DNS server generally takes only a few minutes. Freely available software exists to automate cache poisoning attacks, so an attacker does not need any specialized knowledge or skill (The Internet Infrastructure Foundation, n.d.).

Kaminsky coordinated his July 2008 announcement with the major DNS server software vendors. The vendors immediately issued patches to protect against the vulnerability. Patched DNS servers use TCP source port randomization in addition to the transaction ID to validate responses. This technique effectively increases the entropy of the transaction ID from 16 bits (about 1 in 65,000) to 32 bits (about 1 in 4,000,000,000). Networking restrictions may prevent DNS servers from using the full range of TCP source ports, so even patched servers do not

necessarily benefit from the full 32 bits of entropy. Of course, not all DNS servers have been patched (The Internet Infrastructure Foundation, n.d.).

The additional entropy makes an attacker's job much more difficult, but still not impossible. With current computing power, what used to take an attacker with a single computer only a few minutes would now take months to accomplish (The Internet Infrastructure Foundation, n.d.). An attacker with additional computing power—perhaps commanding a botnet consisting of thousands of computers—could pull off a successful cache poisoning attack against a patched DNS server within a reasonable amount of time. The botnet threat is not merely a theoretical possibility (Rajab, Zarfoss, Monrose, & Terzis, 2006).

Man in the Middle – Packet Interception.

The "man in the middle" attack requires that the attacker has physical access to the network between the DNS client and DNS resolver or the network between DNS servers. The attacker intercepts communications and inserts his own responses in place of the valid responses (Atkins & Austein, 2004, pp. 3-4).

Physical access to the network is the primary barrier to carrying out a "man in the middle" attack. A corrupt employee of an Internet Service Provider, phone company, or cable company would have the necessary physical access. Software and hardware exists to facilitate and automate such an attack. With physical access, carrying out this attack is relatively easy (Callegati, Cerroni, & Ramilli, 2009).

Untrustworthy DNS server.

This vulnerability is due to the fact that the DNS infrastructure involves interaction with DNS servers that are controlled by neither the DNS client nor the administrators of the DNS zone that the client wishes to query. Intermediary DNS servers at the local premises (business,

coffee shop, hotel, airport, etc.), Internet Service Provider, the TLDs, and the root are all potential servers that could be untrustworthy. Travelers with mobile devices (laptops, smart phones) often have little or no control over what DNS servers their device uses. Any DNS server in the chain could have corrupt data, either by accident or intentionally (Atkins & Austein, 2004, pp. 7-8). For example, an Internet Service Provider could have a commercial motivation to use DNS to redirect traffic away from their competitor.

Vulnerabilities in the underlying operating system could be considered a subset of the "untrustworthy DNS server" category. Any DNS server relies on its underlying operating system for its operation. An attacker who can obtain "root" access to a Unix server can control any services running on that server, such as BIND DNS. An attacker who can attain "Administrator" access to a Windows server can in turn control the DNS server service running on that server.

Denial of service.

In this attack, the goal of the attacker is to flood the target with requests, overwhelming the target so that it is unable to respond to valid traffic from other clients. A more advanced version of this attack is the *distributed* denial of service (DDoS) attack, where the attacker commands a large number of hosts in a botnet to attack a target simultaneously (Atkins & Austein, 2004, p. 8). Attackers have attempted D/DoS attacks against the DNS root servers. Root servers have been resilient to these attacks (Castro, Wessels, Fomenkov, & Claffy, 2008).

An attacker's motivation in a DoS or DDoS attack may be simple extortion. An attacker may demonstrate his ability to carry out DoS, and then threaten a company with such an attack unless they pay a ransom.

Example DNS attacks.

In this hypothetical example, an attacker's goal is to obtain login credentials of a bank's customers, and use the credentials to transfer money from the victim's accounts into the attacker's offshore bank account. The attacker himself is located in Russia. The attacker sets up a web server with a web site that has a login page that looks and functions just like the bank's web site. The attacker uses a botnet to attack a DNS resolver/caching server at a major Internet Service Provider in the United States (Kaminsky cache-poisoning attack). The attacker successfully poisons the target DNS server with a DNS record that redirects clients to the attacker's web site. Customers of the ISP attempt to visit their bank web site, but the poisoned DNS server redirects the customers to the attacker's web site which looks just like the real site. When the customers enter their login credentials, the login appears to fail, which is confusing to the customers. In fact, the customers are providing their usernames and passwords to the attacker. Before the customers realize what is happening, the attacker uses their login credentials to log into the victim customers' accounts and transfer funds to the attacker's offshore account. This attack is able to continue until someone reports the problem to the ISP and the ISP clears the compromised DNS server's cache, or until the TTL on the poison DNS record expires.

In this hypothetical example, the attacker is a manufacturing firm in China. The manufacturing firm wishes to spy on a U.S. competitor's e-mail traffic to gain trade secrets and a competitive advantage. The attacker is motivated by profit—millions of dollars' worth of business is at stake. The attacker uses a hidden identity (free Gmail account and a debit card purchased with cash) to set up a caching mail server with a legitimate service provider. The attacker uses public records to determine where the U.S. competitor's authoritative DNS servers are hosted. The attacker bribes an employee of the DNS service provider $50,000 (a year's salary for the employee) to place an invalid MX record in the company's DNS zone (untrustworthy

DNS server attack). The invalid MX record redirects all incoming e-mail for the victim company to the caching mail server. The caching mail server saves a copy of all incoming e-mail before forwarding the mail to the victim's mail server. Employees of the victim company continue to receive incoming mail as normal. The attack continues until someone at the victim's company happens to notice the invalid MX record in their DNS zone or happens to notice that all incoming mail is originating from a single IP address (the attacker's caching mail server) and investigates why.

DNS Security Extensions

DNS Security Extensions (DNSSEC) provides a layer of security on top of standard DNS. DNSSEC uses public-key cryptography to permit consumers of DNS data to authenticate the validity of DNS queries. DNSSEC authentication protects against the threats of cache poisoning attacks, man in the middle attacks, and untrustworthy DNS servers. The original DNSSEC specification (RFC 2065) was published in 1997 (Eastlake & Kaufmann, 1997). That specification was updated in 1999 by RFC 2535 (Eastlake, 1999). The IETF published major revisions to the DNSSEC specifications in 2005 with RFCs 4033, 4034 and 4035 (Arends et al., 2005). These three RFCs define the current basic DNSSEC standard.

DNSSEC-aware DNS servers and DNSSEC signed zones are fully backwards-compatible with non-DNSSEC aware DNS servers and clients. DNSSEC adds additional data to a DNS zone (a significant quantity of new data, in fact), but modifies none of the existing data in a DNS zone. A non-DNSSEC aware resolver will simply not query for the DNSSEC-related data (Arends et al., 2005).

DNSSEC uses asymmetric encryption to authenticate and validate DNS queries. Asymmetric encryption algorithms use a pair of encryption keys—one private and one public.

The asymmetric algorithms and keys permit one person to encrypt data using a private key, and only the public key that is paired with the private key is capable of decrypting the data. It is a best practice to keep the private key offline and secure, to ensure that no unauthorized person may ever use it to sign invalid data. The longer the keys, the more difficult it would be for a malicious person to crack the encryption and compromise the private key (Arends et al., 2005; Liu & Albitz, 2006, pp. 323-326).

The administrator of a DNS zone generates an asymmetric public/private key pair. The public key is published in the zone file as a DNSKEY record. The administrator should keep the private key offline and physically secure at all times. No one other than the owner of the DNS zone should have access to the private key, preventing any other party from forging DNS data and signing it with the private key (Kolkman & Giebman, 2006; Liu & Albitz, 2006, pp. 336-337; Microsoft, 2009, pp. 62-63).

The administrator uses the private key and a software-based utility to "sign" the DNS zone. Ideally, the administrator performs the signing operation offline. The signing process generates special resource records within the zone called RRSIG records. The RRSIG records contain a hash value of DNS data generated using the private key. The original DNS records remain in the zone file in their unencrypted form. Only the published public key which is the other half of the private/public key pair will generate the same hash value, thus validating the authenticity of the DNS data (Kolkman & Giebman, 2006; Liu & Albitz, 2006, pp. 336-342; Microsoft, 2009). Figures 5-9 in Appendix A show an example DNSSEC-signed zone file.

DNSSEC requires a secure method for validating the public key. Otherwise, if someone has access to the zone file they could generate their own public/private key pair and generate invalid signed data. DNSSEC uses a "chain of trust" mechanism to validate public keys. The

public key for a zone is itself signed and validated by a higher authority (Arends et al., 2005). The chain of trust follows the same hierarchy as the DNS tree, so a parent zone validates the public keys of its child zones. The parent zone enters a DS (delegation signer) record for the child zone which contains the child zone's public key. The parent zone signs the DS record with its own private key (Arends et al., 2005; Kolkman & Giebman, 2006).

If DNSSEC were implemented universally, each parent zone would validate its child zones' keys, and only a single public key at the DNS root—a key that is widely known and trusted—would be needed as an entry point into the chain of trust (Arends et al., 2005). In practice, DNSSEC is not implemented universally. The DNS root zone is not yet signed. Only some TLDs are signed, providing a trusted root for zones within the TLD. Isolated segments of the DNS tree with no authoritative parent operate as "islands of security". Each "island of security" must provide an independent, secure means for distributing its trusted root key to partners that wish to use DNSSEC validation. The administrator of each DNSSEC-enabled resolver must maintain a list of Trusted Root keys locally on the DNS server (Liu & Albitz, 2006, pp. 330-333; Microsoft, 2009, pp. 65-66).

The strength of asymmetric cryptography is dependent in part on the key length. Longer keys are more difficult to crack. However, the tradeoff is that longer keys require more processing power to encrypt and decrypt data, and more storage space for the larger DNSKEY and RRSIG records (Chandramouli & Rose, 2006). DNSSEC uses the RSA asymmetric encryption algorithm. RSA uses 512 to 4,096 bit length keys. RSA with a 2048-bit key is estimated to be un-crackable until the year 2035. RSA with a 3072-bit key is estimated to be un-crackable for the foreseeable future (Lee, Malkin, & Nahum, 2007, p. 86). DNSSEC operations anticipate rotating encryption keys on a regular basis—every few months (Liu & Albitz, 2006, p.

336). RSA encryption with 2048-bit or 3072-bit keys provides a very strong solution for DNSSEC authentication and validation—much stronger than the 32 bits of entropy provided by source port randomization.

Signing a zone with DNSSEC also generates another new record type—NSEC records. NSEC records are used to authenticate *non-existence* of a queried record. The signing process generates a NSEC record for each gap between records that exist in the zone. After the last record in a zone, the last NSEC record "loops" back to the beginning of the zone file. When a client queries for a non-existent record "M", they will receive an authenticated response in the form of an NSEC record which states in effect "there are no DNS records between "L" and "P" (Arends et al., RFC 4034, 2005; Liu & Albitz, 2006, pp. 328-330).

The new problem introduced by the existence of NSEC records is that they make it easy to enumerate the entire contents of a signed zone. Many DNS administrators consider this is a significant problem, even though DNS data is by design public and not intended to be private. Before the existence of NSEC records it would be necessary to use brute force to enumerate a zone—querying a zone for all possible values to see what responses the server returns. In comparison to that time-consuming process, NSEC records make it trivial to enumerate a zone (Liu & Albitz, 2006, p. 330).

In response to concerns raised by NSEC records, RFC 4470 defines an alternative called "minimal spanning NSEC RRs" (Weiler & Ihren, 2006; Rose & Nasassis, 2008). This method requires the DNS server to dynamically generate NSEC records on the fly, in response to specific queries. A more widely-accepted alternative, RFC 5155 defines the NSEC3 record (Laurie, Sisson, Arends & Blacka, 2008). NSEC3 records are hashed NSEC records. Hashing the NSEC records provides authenticated non-existence without revealing the exact range of records which

do not exist (Laurie et al., 2008). Minimal spanning NSEC RRs or NSEC3 records enable authenticated non-existence without exposing a zone to the risk of easy enumeration. However, NSEC3-signed zones are *not* fully backwards-compatible with older DNSSEC servers that do not support RFC 5155. Non-NSEC3-compatible DNSSEC servers will be able to resolve queries for NSEC3 signed zones, but will treat the NSEC3 signed zones as "insecure" (Laurie et al., 2008; Rose & Nasassis, 2008).

DNSSEC Administration

Administering a DNSSEC signed zone requires knowledge of DNS, asymmetric encryption keys, and new tools for managing keys and signing zones (Kolkman & Giebman, 2006; Liu & Albitz, 2006, pp. 322-348).

The administrator of an authoritative zone must generate encryption keys and roll over the encryption keys on a regular schedule. The generally-accepted practice is to generate two sets of keys—key signing keys (KSK) and zone signing keys (ZSK). The purpose of managing two sets of keys is that it makes it possible to use different key lengths and key lifetimes. The KSK set uses a longer key and therefore has a longer expected lifetime. The zone administrator provides the public KSK to the administrator of the parent DNS zone. Since interactions with third parties (i.e. the parent zone administrator) are more time-consuming and expensive than self-administration, the KSK changes less frequently than the ZSK. The ZSK uses a shorter key for faster performance, but has a shorter lifetime (Liu & Albitz, 2006, pp. 335-342; Microsoft, 2009, pp. 62-64). The zone administrator might roll over (change) the ZSK every 3 months, compared to a 12-month lifetime for a KSK. (These timeframes are only examples and are not required by the DNSSEC standard.)

The zone administrator must have knowledge of the procedures and technical tools used to generate and manage the encryption keys. Private keys should be kept offline in secure physical storage at all times. Public keys are published in the zone file. Every time new keys are generated (KSK or ZSK), the zone administrator must publish the public keys in the zone file and re-sign the zone with the new private keys. When new KSKs are generated, the zone administrator must provide the parent zone administrator with a copy of the public key and wait for the parent zone administrator to publish and sign the new DS record (Liu & Albitz, 2006, pp. 335-342; Microsoft, 2009, pp. 62-64).

DNSSEC encryption keys have a limited lifetime. The administrator must perform key rollover operations before the old encryption keys expire. Otherwise, DNSSEC validation will fail.

Whenever a DNS administrator adds, deletes, or modifies records in a DNSSEC-signed zone, the administrator must re-sign the zone with the private key. Dynamic update, where hosts are able to dynamically update their DNS records, is no exception. If that feature is enabled on the DNS server, every dynamic DNS update also requires re-signing the zone with the private key. Thus, enabling dynamic update with DNSSEC requires making the private encryption key available to the DNS server software. As mentioned earlier, it is a best practice from a security standpoint to keep the private key offline in physically secure storage (Liu & Albitz, 2006, p. 340; Microsoft, 2009, p. 68).

The administrator of a DNS caching server that is DNSSEC-enabled must manage the list of trust anchor (or secure entry point) keys. The administrator must keep track of the valid lifetime of each trust anchor and update the trust anchors as needed. Failure to update trust

anchor keys will cause DNSSEC validation to fail when the keys expire (Liu & Albitz, 2006, p. 332; Microsoft, 2009, p. 65).

DNSSEC Problems

If DNSSEC solves a real problem, why is it not immediately and widely adopted? Before adopting any technology, most rational persons first evaluate the associated costs and benefits. Even though DNSSEC has been available for more than a decade, the anticipated costs have apparently outweighed the perceived benefits, and adoption has been slow. Some, but not all, TLDs are signed. The root zone is not yet signed (Osterweil, Massey, Ryan, & Zhang, 2008; Osterweil, Massey, Ryan, & Zhang, n.d.; Westervelt, 2009).

Problem: DNSSEC doesn't extend to the client.

How does the end user know that DNSSEC is working? The DNSSEC specifications describe a method for DNS servers to authenticate DNS queries. The specifications do not include a method for the DNS client to authenticate DNS queries, or for providing any type of feedback to the end user. Applications such as web browsers do not provide DNSSEC-related feedback to the end user. This is in contrast to other security features, such as SSL. For example, a user visiting a web site that is protected by SSL can typically see "https" in the address bar and a padlock somewhere in the browser interface. DNSSEC has no mechanism to provide such feedback to the end user (Fratto, 2009).

One could argue that the end user doesn't need to know whether DNSSEC is working at the server level. In the case of a bogus DNS entry, DNSSEC protects the end user by failing to resolve the query. Some believe that from an end user's point of view, it is in fact useful to know that a security feature is working. Feedback to the end user would "close the loop" of communication between the DNS administrator that created the DNS records and signed their

zone, and the end user who issues a query against that DNS zone. Whether or not it provides any "real" additional security, feedback to the end user would provide a feeling of security (Schneier, 2008). Consider the Extended Validation (EV) SSL certificates that turn the address bar green in the Internet Explorer and Mozilla Firefox web browsers. EV certificates provide no better encryption than non-EV certificates containing encryption keys of the same length. Nevertheless, merchants pay a high premium to purchase EV certificates because they believe it makes their customers feel more secure to see the green bar. If DNSSEC had a mechanism for providing user feedback, it may encourage more online merchants to consider DNSSEC as a marketing tool in addition to a security option (Fratto, 2009).

Problem: DNSSEC is difficult to administer.

Deploying DNSSEC involves several steps including generating encryption keys, signing a zone, key management, key rollover, and key distribution. Each step is manually done by a system administrator. It is time-intensive and error-prone. Administering DNSSEC requires specialized skill and knowledge that is not widely available (Friedlander, Mankin, Maughan, & Crocker, 2007; Chandramouli & Rose, 2006).

Consider the steps for deploying DNSSEC for the first time for a zone: First, the DNS administrator generates encryption keys. The general practice is to use two sets of encryption keys, key signing keys and zone signing keys. The DNS administrator uses a software utility to generate the two key sets. The DNS administrator adds the key sets to the zone. The DNS administrator uses a software utility to sign the zone. The DNS administrator replaces the unsigned zone file with the signed zone file. The DNS administrator updates the DNS server configuration to tell the DNS server that the zone is DNSSEC enabled. The DNS administrator provides a copy of the key signing key to the administrator of the parent zone via a secondary

and secure communication method, such as encrypted e-mail. The administrator of the parent zone must include the key signing key from the child zone in the parent zone file. This is where the administration of DNSSEC becomes complicated and un-scalable. The administrative burden on the administrators of the .com TLD would be significant even if a small percentage of .com domain name holders decided to sign their zones. An automated system would be necessary to make DNSSEC administration scalable (Chandramouli & Rose, 2006; St Johns, 2007).

Zone-signing is an on-going administrative task. Every time a record is modified, added or removed from the zone, the DNS administrator must re-sign the zone and re-load the zone file. The best practice from a security perspective is to keep the private encryption keys offline. If that practice is followed, every zone re-signing requires four manual steps: copying the modified zone file to the offline system, signing the modified zone, copying the signed zone file back to the DNS server system, and re-loading the zone file. BIND DNS does support dynamic updates with DNSSEC, but dynamic update requires a security compromise of keeping the private encryption key on the DNS server system so that it is available to the server for dynamic re-signing (Liu & Albitz, 2006; Microsoft, 2009).

Key rollover is an on-going administrative task. The DNS administrator must periodically generate new KSKs and ZSKs. The DNSSEC RFCs do not require a compliant DNS server to warn the DNS administrator when the encryption keys are nearing the end of their lifetime. If the DNS administrator loses track of the encryption key rollover schedule, encryption keys expire, and DNSSEC validation will fail. Every time a key is rolled-over, this requires re-signing the zone with the new keys. When the ZSK is rolled over, it also requires interaction with the DNS administrator for the parent zone, and action on the part of the parent zone DNS administrator (Liu & Albitz, 2006; Microsoft, 2009).

RFC 4986 describes the following requirements for automated Trust Anchor key management (Eland, Mundy, Crocker, & Krishaswamy, 2007): 1. Scalable to meet the demands of the Internet. 2. No intellectual property limitations (i.e., free/open source). 3. General applicability (works with any signed zone). 4. Supports private networks. 5. Detects stale (expired) Trust Anchors. 6. The operator may choose between manual or automated operation. 7. Permits both planned and unplanned key rollovers. 8. Permits timely (quick) distribution of Trust Anchors. 9. Highly available. 10. Supports new RR types. 11. Supports Trust Anchor maintenance (additions, deletes, replacement). 12. Supports recovery from compromise. 13. Ensures authenticity and integrity during key rollover operations. One of the purposes of this thesis is to evaluate whether Microsoft Windows Server 2008 R2 DNSSEC meets any of these requirements.

Administrative tools provided with DNS server software to date do not scale well. DNSSEC specifications do not provide specific standards for administrative tools, so it is up to each vendor to create its own tools. Most are command-line tools. Documentation is sparse. Troubleshooting tools are lacking.

Reverting to an unsigned zone is not a straightforward task.

Problem: zone content privacy / zone enumeration.

The base DNSSEC specifications (RFCs 4033, 4034 and 4035) provide for validated negative responses through the use of NSEC records. A side effect of this new feature is the ability to trivially enumerate the full contents of a zone. This practice is called *zone-walking*. Some DNS administrators consider this a significant security/privacy risk.

There are currently three separate approaches to deal with the zone-walking concern: One approach is the use of NSEC3 records instead of NSEC records (RFC 5155). Another approach

is the use of "minimal-spanning NSEC RRs" (RFC 4470). A third approach is to use split-DNS, keeping private DNS data out of the public DNS (Rose, 2008).

NSEC3 is not backwards-compatible with NSEC. DNS servers that are not NSEC3 compatible cannot validate zones that are signed with the NSEC3 option and will treat the zones as insecure.

Problem: lack of top-level signed zones.

The root zone is not yet signed and only a handful of TLDs are signed (Friedlander, Mankin, Maughan, & Crocker, 2007; Osterweil, 2008). This situation leads to many "islands of security" and makes DNSSEC administration more difficult for the administrators of validating name servers. Many islands of security means it is necessary to configure many trusted anchors.

A workaround for the lack of signed TLDs is to use DNSSEC Lookaside Validation (DLV) as defined in RFCs 4431 and 5074 (Andrews, 2006; Weiler, 2007). DLV is a mechanism for publishing DNSSEC trust anchors outside of the DNS delegation chain. Trust anchors could be consolidated somewhere other than the parent zone. For example, the trust anchor for "example.com" could be hosted by the DLV service provider at "dlv.isc.org" instead of its parent zone ".com". DLV opens up the possibility for commercial service providers to take on responsibility for maintaining trust anchors, instead of or in addition to the TLD administrators.

Problem: additional system overhead.

In comparison to standard DNS, DNSSEC-signed zones require additional disk storage space, network bandwidth, and processor cycles to operate. The additional overhead is significant. The size of a signed zone increases by approximately 4 times compared to an unsigned zone. The longer the chain of trust, the more processing is needed to validate the response to a query (Liu, 2006, p. 335). The additional system overhead makes operating DNS

more expensive. Additional overhead makes the DNS more vulnerable to distributed denial of service (DDoS) attack (Arends et al., 2005).

Problem: perceived lack of concrete threat.

Some argue that DNSSEC is a solution looking for a problem. There are greater risks on the Internet than risks of DNS-related security vulnerabilities. Some examples of the larger threats are application-layer risks, SPAM, and phishing. One could argue that it is more rational to allocate resources towards finding solutions these larger threats, rather than spending limited resources on DNSSEC. One could argue that current workarounds for DNS vulnerabilities—such as source port randomization—are simply "good enough". DNSSEC advocates would counter than the threats to DNS are real and therefore should be a high priority (see infra, Chapter 2, DNS is a Critical Service, DNS Security Vulnerabilities).

When considering whether to deploy new security measures, it is rational to consider the costs and benefits of doing so (Gibson, 2009). In light of the low adoption rates, it is logical to conclude that the perceived threats that DNSSEC protects against are not great enough to justify the administrative costs of deploying DNSSEC.

Consider this from the perspective of a bank operating a web site where its customers can conduct financial transactions. If a DNS cache poisoning attack redirects its customers to a phishing site, the customers should be alerted to the counterfeit nature of the site by noticing the invalid SSL certificate. If the customer falls for the phishing scam anyway, and gives its login credentials to the attacker, is the bank liable for the customer's mistake? If so, what are the projected costs of reimbursing clients for DNS-related phishing scams compared to the projected costs and benefits of deploying DNSSEC?

Consider the perspective of a free e-mail provider, such as Gmail. A DNS cache poisoning attack could permit an attacker to take over a number of Gmail accounts by publishing false MX records that redirect gmail.com e-mail to the attacker's mail server. In turn, the attacker could reset the passwords on the victim's web-based bank account through the e-mail authentication loop. Then, the attacker could remove funds from the victim's bank account. If this scenario occurs, it seems unlikely that Google/Gmail could be held liable for the loss, even though the sequence of events leading to the loss could have been blocked through the universal use of DNSSEC to protect the Gmail mail servers' MX records. In such a scenario, the loss to Google/Gmail would likely be the loss of public confidence and damage to its reputation.

One way to change the results of the DNSSEC cost/benefit equation is to lower the administrative costs associated with deploying DNSSEC. The other is if the perceived security threats to DNS increase. Microsoft has an opportunity to influence the cost/benefit equation by building user friendly DNSSEC administration tools into its operating systems. The announcement of the Kaminsky vulnerability was an example of a change in threat perception. After Kaminsky announced the real cache poisoning vulnerability in DNS in 2008, DNS administrators scrambled to patch their servers with the latest updates to implement the source port randomization workaround. Interest in DNSSEC also increased significantly after the Kaminsky announcement (Morris, n.d.). The United States federal government mandated adoption of DNSSEC in the aftermath of the Kaminsky vulnerability announcement (Evans, 2008; United States, 2009; Chandramouli & Rose, 2009).

Windows Server 2008 R2

Microsoft is a relatively new participant in the DNSSEC scene. The new Microsoft operating systems, Windows 7 and Windows Server 2008 R2 (Release 2), include DNSSEC

features. This is the first time Microsoft has offered DNSSEC support in a client operating system, and the first time Microsoft has supported DNSSEC RFCs 4033, 4034 and 4035 in its flagship server. Microsoft developed these two operating systems in parallel and released both on July 22, 2009 (Rist, 2009; LeBlanc, 2009).

Microsoft Windows controls approximately 90% of the client operating system market (NetMarketshare, 2010) and 74% of the server operating system market (Foley, Feb. 2010). Because of this large market share, to what extent Microsoft supports a technology will have a large influence on the adoption rates for the technology. The default settings Microsoft configures in its client operating systems will have a large impact because most users will not change the default. This is referred to as the "tyranny of the default" (Gibson, 2010). For example, Microsoft Windows operating systems did not have a firewall enabled by default until the release of Windows XP Service Pack 2. Changing the default to firewall enabled made a big difference in the security posture for the majority of Windows users who accept the default settings (Gibson, Jan. 2010).

DNSSEC support in Windows Server 2008 R2 is updated to comply with RFCs 4033, 4034, and 4035. This is the first version of Windows Server capable of signing a zone and performing DNSSEC validation. In comparison, Windows Server 2003 and Windows Server 2008 provided only partial support for the now-obsolete DNSSEC specification RFC 2535. Previous versions of Windows Server could not sign a zone, could host a signed zone only as a secondary DNS server, and did not perform validation (Microsoft, 2009).

Windows Server 2008 R2 includes a new feature called the Name Resolution Policy Table (NRPT). The NRPT is a group policy template that a system administrator can use to centrally configure certain DNS settings for Windows 7 clients, including requiring DNSSEC for

certain domain names. Group policy and the NRPT are available only in a Windows Active Directory environment. The NRPT feature is not available for stand-alone Windows 7 clients. Stand-alone Windows 7 clients must use the Windows registry to configure DNSSEC (Microsoft, 2009).

Windows Server 2008 R2 includes many other technologies which have been part of the Windows Server operating system for some time. These other technologies have the potential to complement DNSSEC. “Dynamic DNS update” is the ability for network clients to automatically add, modify or delete records in the DNS zone. “Secure DNS” is the ability to configure access control lists (ACLs) on DNS zones and individual DNS records. The ACLs control which user or computer accounts are able to make updates. “Active Directory-integrated DNS zones” leverage the distributed multi-master Active Directory database, allowing DNS to use efficient Active Directory replication to keep DNS servers in synch (Stanek, 2008, Ch. 23). “Microsoft Update” and “Windows Server Update Services” offer automated methods for keeping the operating system patched and up-to-date. For example, Microsoft uses Microsoft Update to distribute trusted root certificates (Stanek, 2008, Ch. 2). Windows has an established reputation for providing user-friendly graphical user interfaces and administration wizards. The Microsoft web site www.microsoft.com offers a large library of support documentation (TechNet) and training resources.

Windows 7

Windows 7 is the first “DNSSEC aware” client operating system from Microsoft. The DNS client in Windows 7 is a “non-validating security-aware stub resolver” (Microsoft, 2009). A “non-validating security-aware stub resolver” does not perform DNSSEC validation itself. It is able to request DNSSEC validation from its DNS server. It is able to interpret responses from its

DNS server to determine whether the response is DNSSEC validated. More specifically, the client recognizes the "DO" bit in DNS responses. If the DNS client is expecting a validated response, and the response is not validated, the DNS client will not forward the response to the application (Microsoft, 2009). This provides an extra measure of security compared to a non-security-aware DNS client such as Windows XP or Windows Vista.

The Windows 7 DNS client relies upon its DNS server to perform validation. Therefore, Microsoft recommends using IPSec to secure the network traffic between DNS client and server (Microsoft, 2009). IPSec establishes a secure network connection, ensuring that the client is communicating with a trusted DNS server. Without IPSec, there is a risk of a "man-in-the-middle" attack between the Windows 7 client and its validating DNS server.

In an environment that uses Windows Server 2008 R2 and Active Directory, Windows 7 DNS is also capable of being managed through group policy and the Name Resolution Policy Template (NRPT). The NRPT feature enables system administrators to centrally configure and manage DNSSEC settings for Windows 7 clients that are members of the Active Directory domain. For example, a system administrator could configure a NRPT policy that requires all Windows 7 clients on the company's network to require DNSSEC validation for a specific DNS domain (Microsoft, 2009).

Chapter 3 – Research Questions

The purpose of this research is to test and evaluate whether DNSSEC functionality in Windows Server 2008 R2 and Windows 7 is likely to change the cost/benefit analysis in favor of deploying DNSSEC. Now that DNSSEC functionality is present in mainstream operating systems, does this mean that DNSSEC will become a mainstream security feature? The research will test basic functionality in the server operating system, test basic functionality in the client operating system, test system administration features, and finally evaluate available documentation.

The test lab is a fully-functioning installation of the subject operating systems. A detailed description of the test lab is in Appendix A. The testing procedures are designed to gather meaningful, objective data regarding DNSSEC functionality and administration in the subject operating systems. The detailed test plan is in Appendix B.

Does DNSSEC in Windows Server 2008 R2 Work?

The purpose of this question is to evaluate whether the DNSSEC functionality in the server operating system works as described in the Microsoft documentation. The results are associated with test case 1 in the test plan (see Appendix B).

Does Windows Server 2008 R2 DNSSEC function as described in the Microsoft documentation?

Microsoft documentation for installing and operating DNSSEC in Windows Server 2008 R2 is accurate. DNSSEC does function as described. The DNS server software in Windows Server 2008 R2 successfully functions as an authoritative server for a DNSSEC signed zone. The

dnscmd.exe utility successfully signs a zone. The DNS server service successfully hosts a signed zone as a primary or secondary server.

The DNS server software successfully functions as a caching name server, and it validates queries against signed zones when it has the needed trusted anchor installed. This is true whether the authoritative DNS server is also a Windows Server 2008 R2 DNS server, and when the authoritative DNS server is a Solaris 10 server running BIND 9.

Does Windows Server 2008 R2 address the zone enumeration problem?

The DNS server software does not address the zone enumeration problem. The software does not support minimal spanning NSEC RRs as defined in RFC 4470 or NSEC3 resource records as defined in RFC 5155. The DNS server software is not capable of signing a zone with NSEC3. Microsoft specifically recommends against hosting a NSEC3-signed zone as a secondary server (Microsoft, 2009). If a caching DNS server queries an authoritative zone that is signed with NSEC3, it returns the response as “insecure”. This is not a total incompatibility. The query does succeed. However, the security benefits of DNSSEC are not available to Windows Server 2008 R2 for authoritative zones signed with NSEC3.

Does Windows Server 2008 R2 support DNSSEC lookaside validation?

DNS server software in Windows Server 2008 R2 does not support DNSSEC Lookaside Validation (DLV) as defined in RFC 5074 (Weiler, 2007). Microsoft DNSSEC documentation is silent on the topic of DLV. The lack of documentation for a feature does not mean that it not present. An attempt to use a DLV trust anchor (dlv.isc.org) in Windows Server 2008 R2 failed, verifying that the feature is not present.

How Does the DNSSEC Client Function in Windows 7?

The purpose of this research question is to evaluate whether the DNSSEC functionality Microsoft introduced in Windows 7 has effectively made DNSSEC an "end-to-end" solution. Is DNSSEC functionality in Windows 7 likely to make DNSSEC more of a "mainstream" security technology? The results are associated with tests 2 and 3 in the test plan (see Appendix B).

Does the DNSSEC client function as described in the Microsoft documentation?

The Windows 7 DNS client does function as described in the Microsoft documentation. When Windows 7 is configured to require DNSSEC for a zone, the DNS client does provide a response to the querying application when the response from the DNS server is validated (has the DO bit set). In the same circumstances, the DNS client does *not* provide a response to the application when the response is not validated (DO bit not set).

Does the DNSSEC client provide the end user actionable feedback?

The Windows 7 DNS client provides the end user with no actionable feedback in regard to DNSSEC. The DNS client software does not appear to inform the querying application whether or not DNSSEC validation is in effect. The result is that the end user receives no feedback, positive or negative, regarding DNSSEC. When DNSSEC validation fails, the DNS client simply does not provide a response to the application. It has no mechanism for explaining *why* the query failed. No popup message appears on the screen. No system tray icon provides feedback. No event is logged to any event log.

The lack of actionable feedback limits the utility of DNSSEC functionality in Windows 7. End users have become accustomed to receiving feedback from other security features such as antivirus software, the Windows firewall and SSL. Antivirus software typically notifies the end user with a pop-up message when a virus is detected. The Windows firewall notifies the end user with a pop-up message when it blocks traffic from a new application. Web browsers provide the

end user with positive feedback in the form of a padlock when SSL is in effect. Browsers provide end users with negative feedback in the form of error messages when they detect SSL certificate problems. In contrast, DNSSEC in Windows 7 either works or it doesn't work. When DNSSEC validation fails, the DNS client fails to provide a response to the application. But, a DNS query failure could also have numerous other causes:

- the end user may have made a typo in the hostname
- local network connectivity may have failed
- TCP/IP configuration may have an incorrect DNS server
- TCP port 53 may be blocked somewhere between the DNS client and the DNS server
- The DNS server may be experiencing a problem

The lack of negative feedback makes it difficult for the end user to positively determine that a DNS query failure is due to a DNSSEC validation failure. One option is to reconfigure the operating system to no longer require DNSSEC for the subject zone and try the query again. (If the DNSSEC policy is configured through Active Directory group policy, this will require involvement of a system administrator.) If the query succeeds without DNSSEC then the end user has some evidence that DNSSEC validation is the problem. Another option is to use a network packet capture tool such as Wireshark or Microsoft Network Monitor to capture the DNS query and response packets. The captured packets will show whether or not the DO bit is set in the DNS response. It is likely that an end user and/or the IT support staff would need to spend significant time and effort troubleshooting a DNS query failure that is due to DNSSEC validation failure.

The lack of positive feedback misses an opportunity for Windows 7 to enhance the feeling of security. We use the word "security" to describe a feeling as well as a reality

(Schneier, 2008). If Windows 7 provided positive feedback showing that DNSSEC validation is working, this would result in an increased feeling of security in addition to the reality. The increased feeling of security may in turn provide an additional incentive for companies to adopt DNSSEC. An example of positive feedback that increases the feeling of security is the "green bar" that appears in web browsers when the visited web site has an "extended validation" SSL certificate installed. The extended validation SSL certificate provides no additional encryption strength compared to a regular SSL certificate of the same key length. Most end users do not know the difference between an extended validation certificate and a regular certificate, but they do see the green bar. A site that displays the green bar is perceived to be more secure than a site that does not display the green bar. Companies pay significant dollars for the extended validation certificate because of the feeling of security that end users get from having the green bar appear in their browsers. If DNSSEC provided similar feedback to the end user, companies could use it as an additional differentiator for security-conscious end users.

Is the DNSSEC client easy to configure?

Windows 7 offers no user interface in the Start menu or in the Control Panel to configure DNSSEC. Two options exist for configuring DNSSEC in Windows 7, and neither option could be considered easy. Microsoft documentation states that the options are: 1. Use a Name Resolution Policy Template (NRPT) and 2. Configure the Windows registry key at [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient] (Microsoft, 2009, pp. 79-85). The first option requires an existing Active Directory infrastructure including Windows Server 2008 R2 domain controllers, network, and expertise to administer those resources. This is a significant investment in software licensing, hardware, and technical skills most likely to be present only in a corporate environment. The second option of

configuring the registry is the only option for a stand-alone Windows 7 client. The documentation provided for this option was found to be inadequate. See Figure 4 for a screenshot of the relevant registry keys.

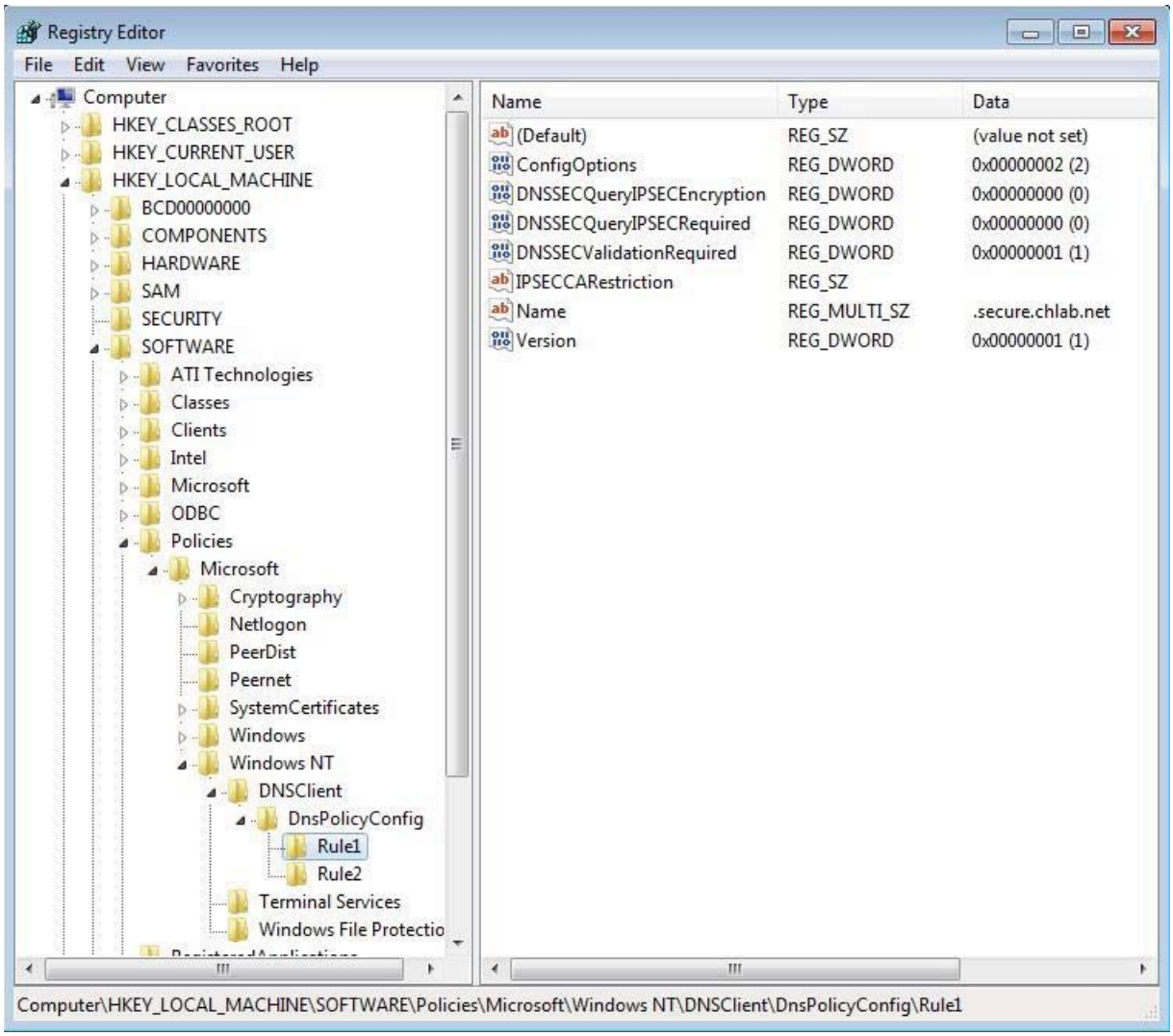

Figure 4. Screenshot of Windows 7 DNSSEC Registry Keys.

It is unlikely that more than a handful of enthusiasts will understand the documentation and actually configure a stand-alone Windows 7 client to use DNSSEC. For all practical purposes, the NRPT is the only option for configuring DNSSEC in Windows 7. The conclusion is that DNSSEC in Windows 7 is available in a corporate network running Windows Server 2008 R2 in

native mode (all domain controllers are upgraded to Windows Server 2008 R2). DNSSEC in Windows 7 is not practical for stand-alone Windows 7 hosts.

Is DNSSEC Administration in Windows Server 2008 R2 User-Friendly?

The purpose of this research question is to evaluate whether the tools that Microsoft provides to administer DNSSEC in Windows Server 2008 R2 ease the burden of DNSSEC administration and thus reduce the costs associated with deploying and maintaining DNSSEC. The results are associated with test 4 in the test plan (see Appendix B).

Is key administration user-friendly?

The first step in administering a DNSSEC-signed zone is to generate encryption key pairs. Key management is an ongoing responsibility for the DNSSEC administrator. All tasks associated with key management are described earlier in Chapter 2. Administrative tools in Windows Server 2008 R2 do not make DNSSEC encryption key management particularly easy.

All DNSSEC encryption key administration in Windows Server 2008 R2 is performed through the command line tool “dnscmd.exe”. Microsoft provides no graphical user interface for administering DNSSEC encryption keys. There is no key generation wizard, key rollover wizard, or key distribution wizard. The server provides no automated method for distributing encryption keys to administrators of the parent zone. Microsoft Windows system administrators accustomed to administering DNS server through the DNS server MMC console will need to learn the command line tool dnscmd.exe. The DNS server MMC has no graphical interface for managing the encryption key pairs. There is no tool for warning the system administrator when encryption keys are about to expire, or to alert the administrator when it is time to perform a scheduled key rollover.

Is zone signing user-friendly?

Zone signing in Windows Server 2008 R2 is similar to key management. All tasks are performed at the command line using dnscmd.exe. There is no graphical menu option or right-click option in the DNS server MMC to sign a zone. DNS administrators accustomed to using the graphical user interface will need to learn the command line tool dnscmd.exe. Furthermore, other than the presence of the new record types, the DNS server MMC provides no visual indication that a zone is signed.

Reverting to an unsigned zone is difficult. Microsoft's recommendation for reverting to an unsigned zone is to keep a backup of the unsigned zone and restore the backup if necessary (Microsoft, 2009, p. 28). This recommendation does not take into account DNS record additions, deletions and modifications that may have occurred in the intervening time between signing and zone and reverting to the unsigned zone. In practice, reverting to an unsigned zone would most likely require rebuilding the zone or manually deleting all DNSSEC-related records.

Is DNSSEC in Windows Server 2008 R2 integrated with other Windows features?

Windows Server 2008 R2 does not integrate DNSSEC with other key Windows features. The Microsoft documentation states that dynamic updates are disabled on a signed active directory integrated zone (Microsoft, 2009, p. 24). Testing also confirmed that when working with a file-backed zone, the DNS server software does not automatically re-sign the zone when records are updated. DNS dynamic update is not compatible with DNSSEC in Windows Server 2008 R2.

DNSSEC is not integrated with the "nslookup.exe" command line tool which is included with Windows Server 2008 R2 (file version 6.1.7600.16385, 7/13/2009). The nslookup tool is not "DNSSEC aware". It provides no usable feedback, positive or negative, regarding whether queries are validated. The tool is not useful for testing or troubleshooting DNSSEC. Figure 5

shows the nslookup result for a query that yields a bogus answer due to an expired signature on the authoritative DNS server. Enabling the “debug” or exhaustive debugging “d2” option in nslookup also provides no DNSSEC-related information.

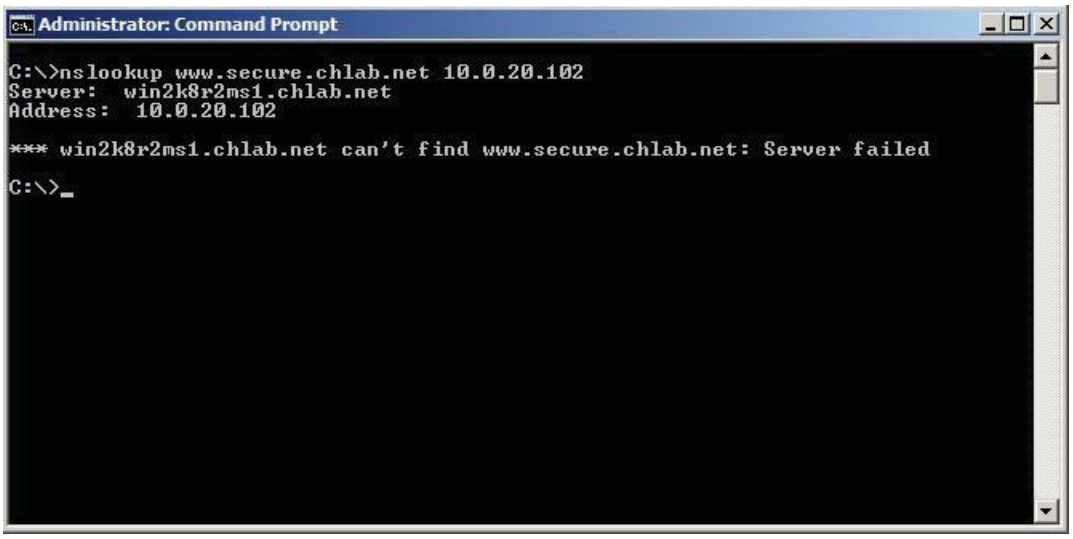

Figure 5. Screenshot of cryptic nslookup error.

DNSSEC is partially integrated with the DNS Server MMC snap-in. The DNS Server “Properties” GUI has a new “Trust Anchors” tab where a DNS administrator can view, add, and delete the public keys of trusted DNSSEC anchors. The DNS Server MMC does not have menu options for generating encryption keys, signing (or re-signing, or un-signing) a zone, distributing keys to the parent zone, or any DNSSEC administration tasks other than configuring trust anchors. Other than the presence of the new resource records in the zone, the DNS Server MMC provides no graphical indication to indicate that a zone is signed or unsigned. The new resource records are visible in the MMC, and the GUI does display the new DNSSEC resource records in a user-readable format if the DNS administrator double-clicks a record to open it (see Figure 6).

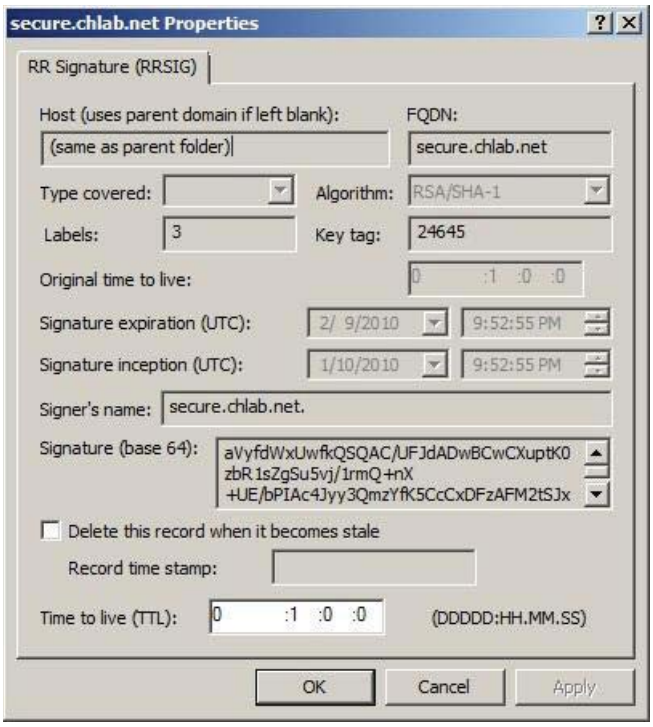

Figure 6. Screenshot of RRSIG record from the DNS Server MMC.

DNSSEC is integrated with the Certificate Management MMC. When the dnscmd.exe tool generates encryption keys, the associated certificates appear in the “Local Computer” certificates store in the “MS-DNSSEC | Certificates” folder.

DNSSEC is not integrated with Microsoft Update or Windows Server Update Services. Windows Server 2008 R2 does not enable DNS administrators to leverage the Windows Update tool for key distribution. Key management for trusted anchors and for signed zones is a manual task.

DNSSEC is partially integrated with the Windows Event Logs. Some events which one might expect to generate an “Information” entry in the logs, but which in fact do not generate entries in the logs, include: generating encryption keys, signing a zone, reasonable advance warning of RRSIG records about to expire, and bogus DNS queries. One event which does generate a useful “Error” entry in the Windows event logs is expired RRSIG records. This event

appears in the DNS Server event log of the authoritative DNS server when a zone is loaded containing expired signatures (See Figure 7). Note, the event does not appear in the log immediately upon signature expiration when the DNS service is running—it appears when the zone file is loaded or reloaded due to DNS service restart.

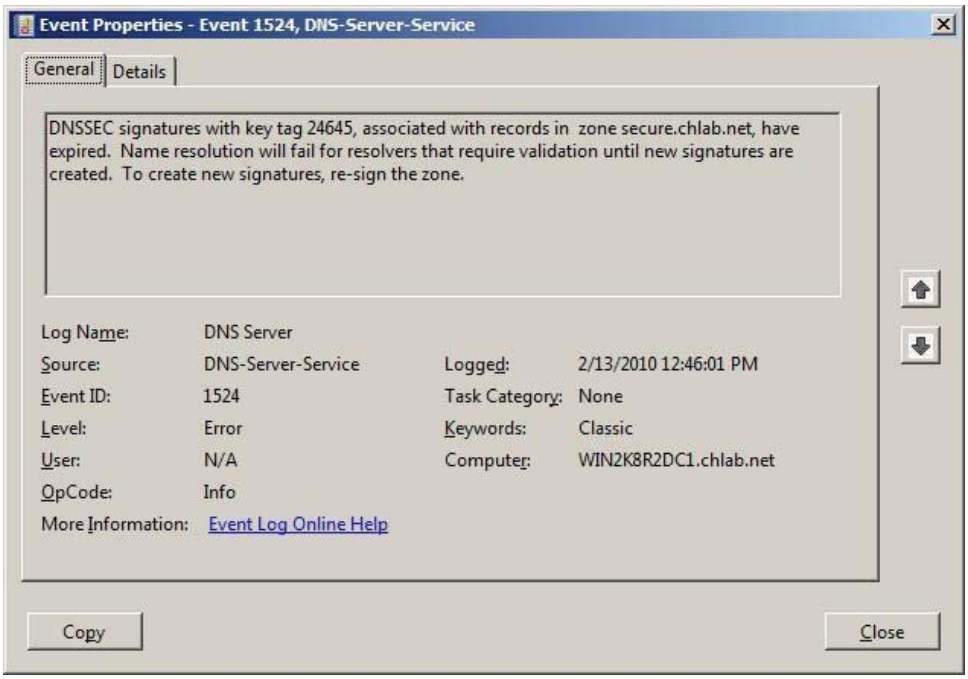

Figure 7. Screenshot of Event 1542 from the DNS Server event log.

Clicking the "Event Log Online Help" link in the event above (see Figure 7) opens the Microsoft TechNet web site with a message "No results were found for your query". DNS "debug" logging is not an option to make up for the lack of DNSSEC related events in the Windows event logs. Debug logging captures raw DNS data packets from the network interface; it does not log DNS service-related events.

Does Windows Server 2008 R2 help prevent common DNSSEC mistakes?

The DNS Server software does not help a DNS administrator avoid the mistake of failing to re-sign the zone after modifying records in a signed zone. The software does not automatically re-sign the zone after the administrator modifies a record. Upon modifying a DNS record, the

software provides no warning, such as a pop-up message stating “This zone is DNSSEC signed, be sure to re-sign the zone after modifying the record!”.

Windows Server 2008 R2 provides the DNS administrator very little assistance in preventing the mistake of allowing encryption keys to expire. The DNS server software does not have an option to automatically generate new encryption keys and re-sign the zone before the old encryption keys expire. The software does not generate any warnings in the DNS server MMC or in the event logs to alert the DNS administrator of encryption keys that are nearing their expiration date. The software does not generate an error upon expiration of encryption keys. The software does generate an error when it loads a zone file containing an expired signature (see Figure 7).

Is DNSSEC in Windows 7 and Windows Server 2008 R2 Well-Documented?

Test 5 of the test plan (see Appendix B) describes the methodology used to evaluate DNSSEC documentation. The Windows 7 integrated Help and Support feature contains no references to DNSSEC. The Windows Server 2008 R2 integrated Help and Support feature contains one article that references DNSSEC. The title of the one article is “New Features in DNS for Windows Server 2008 R2”. The help article does not explain how to configure DNSSEC. The article does contain a link to the Microsoft TechNet web site. If one follows the link and continues to follow links for more information, within three clicks one will find the “DNSSEC Deployment Guide” on the TechNet web site (Microsoft, 2009). The DNS server MMC help file in Windows Server 2008 R2 contains the same article as the operating system Help and Support feature.

The Microsoft web site www.microsoft.com is a resource for Windows Server 2008 R2 and Windows 7 DNSSEC documentation. The TechNet library contains articles describing

DNSSEC, how to deploy, and how to administer DNSSEC (Microsoft, 2009). The primary document on deploying Microsoft DNSSEC is 85 pages (Microsoft, 2009). The document is accurate and a useful guide for setting up DNSSEC. However, no documentation on the topics of testing or troubleshooting DNSSEC in Windows 7 or Windows Server 2008 R2 was found.

The following hypothetical scenario illustrates a problem of the lack of DNSSEC documentation: A DNS administrator who is knowledgeable of DNSSEC may configure an authoritative zone to use DNSSEC. That administrator may leave the company and the company hires a new DNS administrator to take over administering the server. DNSSEC is still a relatively obscure security technology and the new administrator may not be aware of its existence. When the new DNS administrator tries to administer the DNS server he or she will not recognize the new record types. The DNS server MMC is not self-documenting in regard to DNSSEC and has no references to DNSSEC. The administrator may not know the keywords to search for on the Microsoft web site. The administrator will have great difficulty figuring out the purpose and function of the new record types present in the zone. With no user-friendly tools or documentation, the inexperienced administrator is likely to make mistakes that will adversely impact DNSSEC functionality.

Chapter 4 – Evaluate Potential Use Cases for Windows DNSSEC

In light of the above research results, how is Windows Server 2008 R2 and Windows 7 likely to perform in specific DNSSEC scenarios? A January 2010 survey of DNS server software on the Internet found that 79% of the DNS servers on the Internet run BIND and 16% run Windows (Internet Software Consortium, 2010). Does the new DNSSEC functionality in Windows 7 and Windows Server 2008 R2 provide any incentives that might change those numbers?

Authoritative Name Server Hosting a Signed Zone on the Internet

Windows Server 2008 R2 continues to lag behind BIND as a candidate for hosting DNSSEC signed zones on the Internet. It is possible to host signed zones with Windows Server 2008 R2, but it lacks support for features present in the current BIND distributions (Internet Software Consortium, n.d.). It does not support signing with NSEC3 and therefore leaves the zone vulnerable to the "zone walking" vulnerability. Windows Server 2008 R2 has the cost of software licensing, while BIND is open source. Administrative tools bundled with Windows Server 2008 R2 give it no advantage compared to BIND.

Caching Name Server on the Internet

Windows Server 2008 R2 lags behind BIND as a candidate as a caching name server at an Internet Service Provider. It is possible to use Windows Server 2008 R2 in this function, but it lacks support for features present in BIND. Windows Server 2008 R2 does not support NSEC3 records. It will resolve queries against NSEC3-signed zones, however it will treat the zones as "insecure". It does not support DNSSEC Lookaside Validation. Windows Server 2008 R2 has

the cost of software licensing, while BIND is open source. Administrative tools bundled with Windows Server 2008 R2 give it no advantage compared to BIND.

Name Server on a Private Network Running Active Directory

DNSSEC validation functionality in Windows Server 2008 R2 is most likely to be used in an Active Directory environment. In this scenario it is important to distinguish between DNSSEC validation and hosting DNSSEC signed zones. In an Active Directory environment, the authoritative Active Directory integrated zones are not likely to be signed because Windows DNSSEC does not support dynamic DNS. Most large networks utilize DHCP and dynamic DNS. A typical Active Directory environment uses the domain controllers as the authoritative DNS servers for Active Directory integrated zones containing private DNS records. The Windows domain clients are configured to use the domain controller/DNS servers as their primary DNS servers. Typically, the domain controller/DNS servers forward DNS queries for external resources to an outside DNS resolving/caching server. In such a scenario, the Windows administrator may wish to use DNSSEC to validate lookups to the external caching server for certain high-priority domains (e.g. banks, trusted partners). Of course, it is a prerequisite that the high-priority domains are DNSSEC-signed. It is possible and reasonable to configure the Trusted Anchors tab on the domain controller/DNS servers with the trusted anchors for the high-priority domains.

This setup would protect the Windows domain clients if the caching DNS server at the ISP were compromised due to the “Kaminsky” cache poisoning vulnerability. It would protect the Windows domain clients from man-in-the-middle attacks and the untrusted DNS server vulnerability. Any Windows domain client would benefit from this protection, not only Windows 7 clients, because the DNSSEC-enabled Windows DNS Server would refuse to pass along bogus

DNS query results. In the event of a compromised caching name server, when a Windows client attempts to visit the web site of the high-priority domain the query would simply fail, protecting the client from the attack. However, taking the hypothetical scenario one step further, the ungraceful failure would likely result in a phone call to the company help desk. Support staff at the company help desk would have few tools at their disposal to troubleshoot the cause of the failure. Furthermore, the system administrator who configured the trusted anchors on the internal DNS server will need to manually monitor the configuration, periodically updating/replacing the trusted anchors. Otherwise, if and when the high-priority trusted anchors change, name resolution on the Windows 7 clients will fail, resulting in unnecessary downtime for company employees trying to access the high-priority resources.

Windows 7 Active Directory Client

The preceding section described security benefits of enabling DNSSEC validation in an Active Directory environment. In such an environment, Windows 7 clients offer the possibility of adding an additional layer of security. In this scenario, it would be relatively easy to configure the NRPT group policy settings so that Windows 7 domain clients would require DNSSEC validation for the high-priority domains. This would protect the Windows 7 clients from the possibility of a incorrectly configured or compromised domain controller/DNS server. It would also protect mobile Windows 7 clients (laptops) when they are outside the private network. The NRPT group policy settings could instruct the Windows 7 clients to require DNSSEC validation for the high-priority domains even when they are outside of the private network. In such a scenario, if the DNS servers in use are either compromised or do not support DNSSEC, queries to the high-priority domains would fail. This scenario suffers from the same lack of troubleshooting and testing tools.

Windows 7 Stand Alone Client

It is technically possible, but unlikely that a Windows 7 stand alone client (not a member of an Active Directory domain) will use DNSSEC. The documentation is inadequate. Windows 7 does not expose DNSSEC configuration through any user interface other than the Windows registry (see Figure 4). The end user receives no meaningful feedback, positive or negative. Troubleshooting and testing tools do not exist.

Chapter 5 - Conclusions

Windows Server 2008 R2 and Windows 7 are not likely to contribute greatly to the efforts to bring DNSSEC into the mainstream. DNSSEC is an obscure feature of the operating systems and not fully integrated into existing Windows infrastructure. DNSSEC is complicated, making the absence of testing and troubleshooting tools a significant weakness. Windows Server 2008 R2 and Windows 7 do not include administration or usability features that could significantly change the cost/benefit analysis for most users considering whether to deploy DNSSEC.

DNSSEC features in Windows Server 2008 R2 do not compare favorably to the dominant DNS server software on the Internet, BIND. Windows Server 2008 R2 does not support the latest DNSSEC features. Compared to BIND, Windows Server 2008 R2 has the additional cost of software licensing, but it fails to counterbalance the licensing cost by offering advanced administration tools.

References

Andrews, M. (2006, February). *The DNSSEC lookaside validation (DLV) DNS resource record.* IETF RFC 4431. Retrieved January 23, 2010 from http://tools.ietf.org/pdf/rfc4431.pdf.

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005, March). *DNS security introduction and requirements*. IETF RFC 4033. Retrieved September 22, 2009 from http://tools.ietf.org/pdf/rfc4033.pdf.

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005, March). *Resource records for the DNS security extensions*. IETF RFC 4034. Retrieved September 22, 2009 from http://tools.ietf.org/pdf/rfc4034.pdf.

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005, March). *Protocol modifications for the DNS security extensions*. IETF RFC 4035. Retrieved September 22, 2009 from http://tools.ietf.org/pdf/rfc4035.pdf.

Atkins, D., & Austein, R. (2004, August). *Threat analysis of the domain name system (DNS)*. IETF RFC 3833. Retrieved September 17, 2009 from http://tools.ietf.org/pdf/rfc3833.pdf.

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. *IEEE Security and Privacy*. Vol. 7, No. 1, pp. 78-81. DOI:10.1109/MSP.2009.12.

Castro, S., Wessels, D., Fomenkov, M., & Claffy, K. (2008, October). A day at the root of the Internet. *ACM SIGCOMM Computer Communication Review*. Vol. 38, Issue 5, pp. 41-46. New York, NY: ACM. DOI:10.1145/1452335.1452341.

Chandramouli, R., & Rose, S. (2006, February). Challenges in securing the domain name system. *IEEE Security and Privacy*, Vol. 4, No. 1, pp. 84-87. DOI:10.1109/MSP.2006.8.

Chandramouli, R., & Rose, S. (2009, August). *Secure domain name system (DNS) deployment guide*. National Institute of Standards and Technology (NIST), Special Publication 800-81r1 (Draft). Retrieved January 24, 2010 from http://csrc.nist.gov/publications/drafts/800-81-rev1/nist_draft_sp800-81r1-round2.pdf.

Davies, Joe. (2006, April 18). *TCP/IP fundamentals for Microsoft Windows*. Chapter 7 – Host Name Resolution. TechNet Library. Microsoft Corporation. Retrieved April 12, 2010 from http://technet.microsoft.com/en-us/library/bb727005.aspx.

Eastlake, D., & Kaufmann C. (1997, January). *Domain name system security extensions*. IETF RFC 2065. Retrieved Sept. 17, 2009 from http://tools.ietf.org/pdf/rfc2065.pdf.

Eastlake, D. (1999, March). *Domain name system security extensions*. IETF RFC 2535. Retrieved Sept. 17, 2009 from http://tools.ietf.org/html/rfc2535.

Eland, H., Mundy, R., Crocker, S., & Krishaswamy S. (2007, August). *Requirements related to DNS security (DNSSEC) trust anchor rollover*. IETF RFC 4986. Retrieved January 23, 2010 from http://tools.ietf.org/pdf/rfc4986.pdf.

Evans, K. (2008, August). *Memorandum for chief information officers*. Executive Office of the President, Office of Management and Budget. Retrieved October 11, 2009 from http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf.

Foley, M. (2010, February). *Behind the IDC data: Windows still no. 1 in server operating systems*. ZDNet. Retrieved April 1, 2010 from http://blogs.zdnet.com/microsoft/?p=5408.

Fratto, M. (2009, February). *DNSSEC: Forgetting the user, again.* InformationWeek Analytics Weblog. Retrieved October 11, 2009 from http://www.informationweek.com/blog/main/archives/2009/02/dnssec_forgetti.html.

Friedlander, A., Mankin, A., Maughan, W., & Crocker, S. (2007, June). DNSSEC: A protocol toward securing the Internet infrastructure. *Communications of the ACM*, 50(6), 44-50. DOI:10.1145/1247001.1247004.

Gibson, S., & Laporte, L. (2009, December 31). *The Rational Rejection of Security Advice*. Security Now!. Episode # 229. Gibson Research Corporation.

Gibson, S., & Laporte, L. (2010, January 21). *Listener feedback #84*. Security Now!. Episode # 232. Gibson Research Corporation.

The Internet Infrastructure Foundation. (n.d.). *KaminskyBug!SE*. Retrieved October 11, 2009 from http://www.kaminskybug.se/index_en/.

Internet Software Consortium. (n.d.). *BIND 9.7.0rc1*. Retrieved January 22, 2010 from http://oldwww.isc.org/sw/bind/view/?release=9.7.0rc1.

Internet Software Consortium. (2010, January). Internet Domain Survey, January, 2010. Retrieved April 17, 2010 from http://ftp.isc.org/www/survey/reports/current/.

Kolkman, O., & Giebman R. (2006, September). *DNSSEC operational practices*. IETF RFC 4641. Retrieved January 22, 2010 from http://tools.ietf.org/pdf/rfc4641.pdf.

Laurie, B., Sisson, G., Arends, R., & Blacka D. (Feb. 2008). *DNS security (DNSSEC) hashed authenticated denial of existence*. IETF RFC 5155. Retrieved January 23, 2010 from http://tools.ietf.org/pdf/rfc5155.pdf.

LeBlanc, B. (2009, July 22). *Windows 7 has been released to manufacturing*. The Windows Blog. Microsoft Corp. Retrieved April 1, 2010 from http://windowsteamblog.com/blogs/windows7/archive/2009/07/22/windows-7-has-been-released-to-manufacturing.aspx.

Lee, H., Malkin, T., & Nahum, E. (2007, October). Cryptographic strength of SSL/TLS servers: Current and recent practices. *Internet Measurement Conference*. Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. New York, NY: ACM. DOI:10.1145/1298306.1298318.

Liu, C., & Albitz P. (2006). *DNS and BIND*. 5th ed. Sebastopol, CA: O'Reilly Media Inc.

Microsoft. (2009, October). *Understanding DNSSEC in Windows.* Microsoft, Inc. Retrieved February 6, 2010 from http://technet.microsoft.com/en-us/library/ee649277%28WS.10%29.aspx.

Microsoft. (2009, November). *DNSSEC deployment guide*. Microsoft, Inc. Retrieved December 27, 2009 from http://www.microsoft.com/downloads/details.aspx?FamilyID=7a005a14-f740-4689-8c43-9952b5c3d36f&DisplayLang=en.

Morris, S. (n.d.). *A favorable year for DNSSEC*. The Internet Infrastructure Foundation. Retrieved October 11, 2009 from http://www.iis.se/en/domaner/dnssec/ett-bra-ar-for-dnssec/.

NetMarketshare. (2010, March). *Operating system market share*. Retrieved April 1, 2010 from http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8.

Osterweil, E., Massey, D., Ryan, M., & Zhang L. (2008, October). *Quantifying the operational status of the DNSSEC deployment*. IMC '08. DOI:10.1145/1452520.1452548.

Osterweil, E., Massey, D., Ryan, M., & Zhang L. (n.d.). *SecSpider the DNSSEC monitoring project*. UCLA. Retrieved January 24, 2010 from http://secspider.cs.ucla.edu/docs.html.

Rajab, M., Zarfoss, J., Monrose, F., & Terzis A. (2006, October). *A multifaceted approach to understanding the botnet phenomenon*. IMC '06. Rio de Janeiro, Brazil. DOI:10.1145/1177080.1177086.

Rist, O. (2009, July 22). *Windows Server 2008 R2 reaches the RTM milestone*. Windows Server Division WebLog. Microsoft Corporation. Retrieved April 1, 2010 from http://blogs.technet.com/windowsserver/archive/2009/07/22/windows-server-2008-r2-rtm.aspx.

Rose, S., & Nasassis, A. (2008, April). Minimizing information leakage in the DNS. *IEEE Network*. Vol. 2, Issue 22, pp. 22-25. DOI:10.1109/MNET.2008.4476067.

Schneier, B. (2008, January 21). *The psychology of security*. Retrieved April 12, 2010 from http://www.schneier.com/essay-155.html.

Stanek, W. (2008). *Windows Server 2008 Inside Out*. Redmond, WA: Microsoft Press.

St Johns, M. (2007, September). *Automated updates of DNS security (DNSSEC) trust anchors*. IETF RFC 5011. Retrieved January 22, 2010 from http://tools.ietf.org/pdf/rfc5011.pdf.

United States. (2003, February). *The national strategy to secure cyberspace*. Retrieved September 22, 2009 from http://georgewbush-whitehouse.archives.gov/pcipb/cyberspace_strategy.pdf.

Weiler, S., & Ihren, J. (2006, April). *Minimally covering NSEC records and DNSSEC on-line signing*. IETF RFC 4470. Retrieved Jan. 23, 2010 from http://tools.ietf.org/pdf/rfc4470.pdf.

Weiler, S. (2007, November). *DNSSEC lookaside validation (DLV)*. IETF RFC 5074. Retrieved January 23, 2010 from http://tools.ietf.org/pdf/rfc5074.pdf.

Westervelt, R. (2009, September). *DNSSEC deployment challenges can be overcome*. Searchsecurity.com Security News. Retrieved September 14, 2009 from http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gci1367915,00.html.

Appendix A – Test Lab

The Hardware Platform

The hardware platform for the virtual test lab is a Lenovo T500 notebook computer with an Intel ® Core ™ 2 Duo 2.80 GHz 64-bit processor, 4.00 GB of RAM, and a 250 GB SATA hard drive.

The Software Platform

The host operating system installed on the Lenovo T500 notebook is the 64-bit version of Windows 7 Professional. Windows 7 has Internet access through a wireless network connection to the author's home network. The Internet Service Provider is Qwest.net DSL. The Qwest.net DNS servers are at 205.171.2.65 and 205.171.3.65. Windows 7 is updated with all security patches as of April 2010.

The virtual machine manager is Sun VirtualBox v. 3.1.6 r59338. The test lab has four guest virtual machines configured to run in VirtualBox, as described in Table 1.

The three Windows virtual machines are configured as an Active Directory domain, chlab.net. The domain controller has a group policy object configured with Name Resolution Policy Table (NRPT) entries. The NRPT configuration requires that domain workstations request DNSSEC validation for any queries in the zones secure.chlab.net and secure.chlab2.net (see Figure 16).

The DNS Architecture

The test lab has three DNS Servers and three DNS zones, as described in Table 1 and Figures 4-11. The key-signing key and zone-signing keys used to sign the secure.chlab.net have the maximum 4096 bit length.

Table 1: Test lab virtual machines

Hostname	WIN2K8R2DC1	WIN2K8R2MS1	WIN7	SOLARIS10
Role	Active Directory Domain Controller; DNS Server; Group Policy	Active Directory Member Server; DNS Server	Active Directory Domain Member/Client	BIND DNS Server
Operating System	Microsoft Windows Server 2008 R2 Standard version 6.1 (build 7600)	Microsoft Windows Server 2008 R2 Standard version 6.1 (build 7600)	Microsoft Windows 7 Professional version 6.1 (build 7600)	Sun Solaris 10
64-bit OS?	yes	yes	yes	yes
Allocated Memory	1024 MB	1024 MB	1024 MB	768 MB
Network Adapter 1 (uses NAT to access external resources, the Internet)	static IP 10.0.2.101 mask 255.255.255.0, gateway 10.0.2.2 DNS [none]	static IP 10.0.2.102 mask 255.255.255.0 gateway 10.0.2.2 DNS [none]	static IP 10.0.2.103 mask 255.255.255.0 gateway 10.0.2.2 DNS [none]	static IP 10.0.2.104 mask 255.255.255.0 gateway 10.0.2.2 DNS 205.171.2.65 205.171.3.65
Network Adapter 2 (internal network for virtual machines to communicate with each other)	static IP 10.0.20.101 10.0.20.111 10.0.20.112 10.0.20.113 mask 255.255.255.0 gateway [none] DNS 10.0.20.101	static IP 10.0.20.102 mask 255.255.255.0 gateway [none] DNS 10.0.20.101	static IP 10.0.20.103 mask 255.255.255.0 gateway [none] DNS 10.0.20.101	static IP 10.0.20.104 mask 255.255.255.0 gateway [none] DNS [none]

Table 2: Test lab DNS Servers and Zones

DNS Server	WIN2K8R2DC1	WIN2K8R2MS1	SOLARIS10
DNS Server software	Windows Server 2008 R2	Windows Server 2008 R2	BIND 9.3.6
DNS Server is primary authoritative for:	chlab.net (active directory integrated zone) secure.chlab.net (signed, file backed zone)	[none]	secure.chlab2.net (signed zone)
DNS Server is secondary authoritative for:	[none]	[none]	[none]
DNS Forwarding	yes	yes	yes
DNS Forwarders	205.171.2.65 205.171.3.65	10.0.20.101	205.171.2.65 205.171.3.65
DNS Recursion	enabled	enabled	enabled
DNS Caching	enabled	enabled	enabled
Trusted Anchors		secure.chlab.net secure.chlab2.net	

```
;
;  Database file secure.chlab.net.dns for secure.chlab.net zone.
;      Zone version:  6
;

@                       IN  SOA win2k8r2dc1.chlab.net. hostmaster.chlab.net.
(
                                    6            ; serial number
                                    900          ; refresh
                                    600          ; retry
                                    86400        ; expire
                                    3600       ) ; default TTL

;
;  Zone NS records
;

@                       NS    win2k8r2dc1.chlab.net.

;
;  Zone records
;

@                       MX    10    mail.secure.chlab.net.
mail                    A     10.0.20.111
www                     A     10.0.20.112
```

Figure 8. Zone file for secure.chlab.net unsigned zone (1 KB).

```
;
;  Database file signed.secure.chlab.net for secure.chlab.net zone.
;      Zone version:  18
;

@                       IN  SOA win2k8r2dc1.chlab.net. hostmaster.chlab.net.
(
                                    18          ; serial number
                                    900         ; refresh
                                    600         ; retry
                                    86400       ; expire
                                    3600      ) ; default TTL

;
;  Zone NS records
;

@                       NS    win2k8r2dc1.chlab.net.

;
;  Zone records
;

@                       MX    10    mail.secure.chlab.net.
@                       RRSIG SOA 5 3 3600 20100209215255 (
                                    20100110215255 24645 secure.chlab.net.
                                    mCogRCrz+DCWdNRiNgqYBYzk22tpRE3w6DWn
                                    Yyx09EZ9YAYLQXwxgXS35zdCtIq4qkBsVo6b
                                    bifs2WKvzh7+01NWlWvwICaBYE3MRIJPRw7n
                                    UW9kUw+Okg4TP8rl6THMepZTfEnmm1cCQ0yv
                                    bPhZN6gc6K5TJBTN6JLaWgrQJ8xfUO+DxYwS
                                    IiKjeQS7EueykGKiHOUaIlWpT1J9PB+DYyBi
                                    woiekeg35z3LrJI9rdmIB1DsFRIK92ztKlHS
                                    1Be3PphLBaXxlvpIxBnMSPZEIRpGZ/+Yc2Zn
                                    Uh6XXmT3i+VUG7UJOdCQFts3jSOwhxvYqGg7
                                    YSf3RthHQqflksxsRvTb0Ot9ALRmK0b6bViO
                                    AQi1z5Wlt9AT2MCHPNAAPAT4Kejdb1fIWL5z
                                    KiPaMhDKcjzZprAwuiSanqk6hTyVpTP4oE1M
                                    HO8dNOL2z3PcE5kT6hDxaynZg+PTm4zAJWhN
                                    ISWhSqw8elmw6ttIVq4UiJfsSzTZOB2yBroc
                                    tdNlvK5W72XgAKxwOu3JZIe/qRsbmqbPFbRX
                                    wFgQtCLMvZJ0BzoT5VhJ727nj9rAc7ZfXWJL
                                    8wlonRxpz7zc70mU9dTL9pdQo4aY0O7sPXJy
                                    um+XkK/QpfsWDHj99GUCJ5iK1YfBpXNz5xz2
                                    tScGJAijKlu9E+rITiZINwzRTOOSLzKg/bo=
                                    )
@                       RRSIG NS 5 3 3600 20100209215255 (
                                    20100110215255 24645 secure.chlab.net.
                                    c46C86e2HdSKN3MhnvL1Bf7naKmKUQNYSc0E
                                    s4ZjhG5z6j+jp415ymlVepMqQEFhr0kNX+dH
```

Figure 9. Zone file for secure.chlab.net signed zone (16 KB), part 1 of 5.

```
                                        YU/nuLmPFOTZ2Rn7crvGws+BMUTC87hcIsjt
                                        11fPB0xpszUB3heC0dsv+AICBzub5MHlUnxQ
                                        GGDw+UO2wGQfMtj5lMq9wS1CWr9XgQqkLd/H
                                        SCANi3QA8pWblCqCF8NgMFcpkNNpwJCwwI0c
                                        5z7h4X2xiK5LNbEeg4r8wbTJmRS4kq3illOd
                                        GMUA+evXWUWd+bmHBHsxo2pDpc7VMjJqNy8q
                                        6MicWNr9v0tFYz/ZzZ/Ed2hf7lG9tr9cO0U=
                                        )
@                       RRSIG MX 5 3 3600 20100209215255 (
                                        20100110215255 24645 secure.chlab.net.
                                        pqktF6t1RILOwx7SrPiFLsqsMo+zoKmz/2Le
                                        QXkoNiacyEz45h5NXvkAyK8xCNxdJJSiaoWx
                                        ANxKtx+3FeHBdT43Dqd95+Li0vsY9tRrgLi+
                                        cd5Hl6Xtf5+bQKgDkTBwL5rY6sFIQ6Z+ZIws
                                        UtNZSQdfzEG981mST+OzP+47s5y90bIu1ncW
                                        EV/DJ5HpLjjBQ6lr06MwthVN9b8OIFPQxbJU
                                        c2oJiaU8gkUxryRqizBusIzzos5PgWVgY1Jt
                                        fUCgLDE9xcAyLiECwA8AAgeh+JGVsb0/uYWa
                                        H75wBn6GFNrom6SDODZKABX3+D9hFL0Ql/OD
                                        xC3V79TgoJxqSH6FGYokjeRPAXe77NtHDOpQ
                                        Erzcdcx1u8LDFyZr5U5eff3j6IWTcPrSNLP/
                                        m9ekNG7bbMjlFsk+QLwU3VDXEkTREhnzUHoe
                                        sNrbDP9DxFSwlJ5YGOeGtKdf1QP4UyrWdkwL
                                        +cMt+7YRpf6s4nx6kYP1UiMw3djyO/2HKZjF
                                        he8PFki62fQumGkWbTTfA0r2ntopqoBoCf2U
                                        Wd7szjxUJ2y6zzTtvPodKg6XsiF8j7bvpyS0
                                        ukkMnQbW7+WFaOh0nJcsyR5jTjZsILHgfU8a
                                        d0NEk6Trbwn6DdJWx+gHt4J3xUBT9Dv79718
                                        5ANXHgYTz4GzoMtgKA4Bl+d54KE+tlLjEeA=
                                        )
@                       RRSIG NSEC 5 3 3600 20100209215255 (
                                        20100110215255 24645 secure.chlab.net.
                                        C981ejcXKzUZlf8cWm7scElR2FJBPSsTdG/g
                                        QJgQ3oV2bRJKin2c/S17zoL3anx+2m4Pz1wS
                                        XNRE5/9dwkw7yPhYUx2z+neCqb9bj6JcpUQM
                                        +Qgj/3AWCNOGWruzQuQ99kuvu5wVVW6w5B0g
                                        /sbqqlbHYpnQo2cyOt6oRYkNbW68uJxd0ug6
                                        vgot32W5u1B/UxLYhdRudI3V9CHcApSIYL9R
                                        TqBtQL6DtAgmgNjBSiwRwkLpz1Xg44jRwjHB
                                        bxVDHgsStP9qWMCKKMYoAsdx90oTibJ/z9Kk
                                        Iw0E2Hn285CJ4J8rL+8Af9d5/jopdxSH40cM
                                        fnEAncJRq1tZ+9tAl2j81Lt8jXzWx46SVJ3r
                                        JMODFW3irxxQpJrQq0NPgK8lshosa32QH9MZ
                                        ZKzsDHUtafkvthF8+ZBoyYq7PfARByZKQkMe
                                        UwV9CnIQGhT/A6j2HlX8MraXgYLTRyeyb94U
                                        I4em3c16hHdL/NefdZuhToM+9+TF56xWktty
                                        dlg5AqbxcYVZJKWekBfFViZ0QGi3xlKMdvgl
                                        r3DiQndGPUqvnVv6+cPNbgmdmkANg9xqjszK
                                        pcsD4DXjCYcjWcScHS/Viroqxb0rcjrZaZDL
                                        fn8QRNF5PrlWcpLaMI9rRLDr9z1GM81lQxRm
```

Figure 10. Zone file for secure.chlab.net signed zone (16 KB), part 2 of 5.

```
                                        6iFQ4vI+ariZQX7O2jNWdXdOSCVszmC6rzBO
                                        VAykaQG5BiUxwx65kI7qEFsdccqkU2Mq72zS
                                        aZ6XxevfdCbSMMbv9+0MiB6Ojuoui/o4V+th
                                        g4ZVxDXwGSYDeNCCqPS/mmu92U12uSC86z5f
                                        9R9mYE1LshxB4iG1GAfPCV9KQ0g6lpjIYojX
                                        S1CqyevvopiUEYajOtOBX8++iHq+o4J9KAu8
                                        3QA6TUUZGsBDinUYDpO78EFYJL5IBnL0CxP5
                                        +s+sUqRtXk+lZSVO9WvCzx73hjenPejyiOA0
                                        2aeaTQjKaxp2B/YOsOgRZOno24ZlmbFGNWTD
                                        GLzbORGksOz6S3a+0v6eUrRfhKeaW972ilsU
                                        3a9Y+7jP/A6JJ/x0jqSw5VXxfZH8M8rHVs1B
                                        Xe8JN2VAmyJE9nshcDXuSH1FF7d7aIct/nZj
                                        NCqeNSNw0kiFrGQ+Z/nJ//db2pEcKrNTYs2E
                                        D4ktMPpSAbvguJWrVcvIdc6bsILqPu+5FfQ=
                                        )
@                       RRSIG DNSKEY 5 3 3600 20100209215255 (
                                        20100110215255 24645 secure.chlab.net.
                                        aVyfdWxUwfkQSQAC/UFJdADwBCwCXuptK0zb
                                        R1sZgSu5vj/1rmQ+nX+UE/bPIAc4Jyy3QmzY
                                        fK5CcCxDFzAFM2tSJxpv+U8uKaTFR8LUz4YC
                                        rBJ9QT0pgkiQLmU2KbSMW2i4UOQzKsjIehmM
                                        pkT2OsUFUrIWKtsyynwKHwqqTs3jDJKOPGy8
                                        9uNwGHMvnaTWy3F+qPVc1uQLJI/X9yC5mTIi
                                        B3j6SKzq/8K5og3oxGKA8n9Muy/bRs+2nf5V
                                        j8kgT2QAj2SBfvi+VFHTqVlZHvWra/3D3cID
                                        vPntqbMeshFY42OggUXlDxR7J9jpn/O7+qIc
                                        88pqCZMLCU74KHR9jw/+N8eVU+EVK8fUhnRg
                                        hY29eOeIXFXzY5gX3kvgM1nHPZyEPb0tj/up
                                        /vRij5NWoGEp0kaNxgNeV9wTYciLqBb9lM+W
                                        rUVRoN5o6iYv10Azrly7nEL8SrVf1/nyCCT5
                                        I9yLWxtFiyL4K95597YIBR/EGVYYRiNRwBZk
                                        kzvPoVBLk07iOTHPxcxuc4+aC0AGOFIBoPub
                                        HFVt4GYmA5XpP9EFv8eEG6RLUbF8U9lwk0z9
                                        z3ftg5PZPFCHRDWws2b+Qe+E1DYsj7xUsJMe
                                        2wi+BZ3FRIspBBAR4ys0YIgQYxdBrc/kCiYB
                                        EkWPP/13Xt7b76p6QE1rDf3FQRnseUtnzYE=
                                        )
@                       NSEC  mail.secure.chlab.net. NS SOA MX RRSIG NSEC
DNSKEY
@                       DNSKEY      256 3 5 (
                                        AwEAAbDCPKM+ej4HPCjvoVqz60+YNtcQbnmi
                                        yyrjPh/y5uGAYgYCAntgf/ildqZj6P8yoI3C
                                        SKnL4eEM4WGCbmLE4NYpMad+DWb9RJFH+oZZ
                                        psbvQHtcELw9IXm69wOLtrLcSU3jtq9t2GBu
                                        kv9v2CRp9uJG6ZL3tEa1q35Uhu9ReXh1EOgV
                                        MRXgNlY96oRuvWlcC8BJRJ/jCTIMORi4B37j
                                        NKqxauQ9CeJfLU802aIb0rGm8/LGERivYCsf
                                        BM7v37CanDe3BCbOVL1jrckXLtZb9jV1jago
                                        eLz9J5dc7M0NwZHxnMGgHEHr9aeYn5A+O930
                                        ZWq/B7Dp6s8Mzxn1awqmz6AzkksfYMpTSGji
```

Figure 11. Zone file for secure.chlab.net signed zone (16 KB), part 3 of 5.

```
                                    45DJ
                                    ) ; key tag = 24645
@                       DNSKEY      257 3 5 (
                                    AwEAAeu2+yxFHn/E8EAZN7lLJ7nrhWyPiurs
                                    yuiHnxA8zyU55mGDM/yIHJ/dFNEzdsn2Ytp5
                                    QQ3ysnEuUdR+OYkPnoISeY2ozHUjLg8m8Tfy
                                    lXNvddMFW5Qunfogh+FNNQuHYsfpFjXM2eDt
                                    cTVejCHikkREbEERbhcI+gJAVLu+PkBMnxyW
                                    UyDME52AIY42HUcLAwBZZKg4MOB+pENIQBvB
                                    GPthrTXGkleKcNxRGCRZDXlKgSPxf+voXfr8
                                    deyBTQY13x03Tf1k+4nZYhANCFbw39MyfMHc
                                    CmFHpUTq2G3QCxl1D6kMRflpxrDVgxIhmUYz
                                    HKxGGuxoQuGQO3FB+21IIN5z3sZGJFKEkyxO
                                    VoBqX4cn8GGUj6BmhwJhiwQhe+AjiZkGQb9G
                                    GG9yroOjtKh8rJheCCC1oCGCZClIlXBXln10
                                    ZTtO/UxKNckXEMQlglzrbL4X9nd3HlGviEZC
                                    jlNuKQpCV0X+9MmKcDhK9/rseltz+ZsUW62U
                                    3mJRx106eiXzhI/gt82s1V1ts4MasmYSapV7
                                    eZOqC2vOB3E8G4ZC4lp4m6U3arJ1NqRGnC55
                                    zzZv5PKa6sefX02YnSDguvG3a9nYAtGDj4Xz
                                    /1AdXt3vMbjrfvtEM3gsB4ePJoUDN3TpvTW8
                                    dZhNuzrLNuQyz7CNMGSdYE9xwNQcI7x89+mE
                                    g2ad
                                    ) ; key tag = 62944
mail                    A     10.0.20.111
                        RRSIG A 5 4 3600 20100209215255 (
                                    20100110215255 24645 secure.chlab.net.
                                    mTLSg41aBFBw0GyaQViaUV9rsuWcP5xZg87/
                                    eogCmpfndO66wKRmfODfev6ozfMw+TVnuNW9
                                    /sb+CNK/LUYaf5DIc1yhCkYoeQQroFwiERa+
                                    dNBdR2eOG4uN3TVdHTyNgPAO3rHgEYGShf5P
                                    Ge+xGQBfy9BciY1eDrYkmYIGOdsFI+d0QTGA
                                    7dP58fFu6MEPs6j80Qw2i+nUPL/9iJeDteBb
                                    jR59zcTwRtwVgFVCjR/SmeoW+DgLxIqGtyuS
                                    gdx/C5rQ1qiN74CiZgOS+O/MBypRjulGE5C3
                                    TfIAoaEKWLc8l7s604Hpgx5iLUwG9XSh3eBj
                                    dk4NikzvMtjbGuGQWGalc7GXA/amzC1ye4Qk
                                    GzeTSFml4onatLKSfPQ4UJlWsgvHi/ZvMCEP
                                    UoNAWPcLnkD8KmmCdPNpV3ltyOpMttGbAJlB
                                    rnMWR59JGULB9R/6xl1RFeo/P1pARAbDilqZ
                                    YOy9UcxKtjDCi01gIRiWFH2/tQBnrhqKGxpU
                                    +nhyhWbvbZ1JtGo7JwDD4mdxuO3irr2Xfl54
                                    w06dEoPD1RXwsGKTOAfpfLGk+FiBw2adjc9m
                                    Uw5wgBk6cfhLfiHLoHXWVrl+f6c9d3jWAXlL
                                    QjDrlbvhrgpWafZcBj8hOPCidBTE52VRttsz
                                    DerBV/xzigABmqTRlWjhARqgraLJALOTaqk=
                                    )
                        RRSIG NSEC 5 4 3600 20100209215255 (
                                    20100110215255 24645 secure.chlab.net.
                                    A4lBEKQVlak2bwqt8YVrFR/+/u8Adz3mNW01
```

Figure 12. Zone file for secure.chlab.net signed zone (16 KB), part 4 of 5.

```
                                meMYF+hD7bumB0M+c/uUg0fCZb79GpwqLWZY
                                KS0pqloPyWg0tNvJhtKS/vtDanH+7LaVwOzN
                                9BVISgbsvrWcyApqZTiX6HFQsgkkQaPbOqwf
                                ejnj/EV/F5HxaxtIL+XRmjs2r3eASOez1til
                                0GUxN+6atnxNsAbWqP03FUfySJDa+5/9wmgo
                                fZ7+WLKlZcwOlHrUGI6OiWdG74XpM0jfT0Nl
                                TumBwcoALdHP0RO/rPsI+mDtxC5MIdusvY6D
                                R5RJqVQY5SrC5rY/idAZamLEoQKBXeMCZy8Z
                                zwOYPdndWz7mS9d6j09PBSCu0NYZwq2hoEQ=
                                )
                        NSEC  www.secure.chlab.net. A RRSIG NSEC
www                     A     10.0.20.112
                        RRSIG A 5 4 3600 20100209215255 (
                                20100110215255 24645 secure.chlab.net.
                                Rvt+0/dPDzgAP2AwS0dc4j2LrWzwH4OHqqtH
                                jb5CGQaFEVmksgmdmtjeei8Pm3bXuSZxxWI7
                                ESPrqf9UmKLd3D45RmCx0Y+4Om8Pr0SBeNeK
                                KCiGWQXl/wVzFT/mlDfxBx26B5mxMLFFpbX0
                                mp7OMlyn8wTmcfnpILW39n4t0XP83IVIXd0a
                                1laztC4jNpGwAGi2EFHigttXXu0/BJv2D1Rm
                                y5v/tSo938TnEYycIQs0Am/QfAuSwbIJ+/kO
                                sPoKDYFsWkVyPyWGaufBAqNbGJJXD6KpBGR7
                                +E/ea6YcDoUXgRIe1iQCeV16AIFxsrUUwmpX
                                O7kqqZlUckLFtG6jLMbTcDc3dPH5t9/wK+Bg
                                bGuEbPgv+UClYdSknsJUCSwxTFZlVhNL6wZ3
                                K0wicNu+rcYKQMpxv67A6yQ9jyX+ZJxAyevL
                                iO8ysVt5iRpx8GsquPqEEX+HAbgTRu9cChOe
                                Tuhc82I8QxK3V3oJvkSZJbBOoXn3gFEvf72I
                                RUcv2ATMjZ4odPoa/XLbAwousVQ/Z4YDZX+q
                                7TX3H/jzY1RQC0s9ZzKDSa7sXNkJzavjbRT1
                                iVA2zh2hTVMqkSdrTHU4i82UAcWropi2uH8f
                                FZhsMlw2kdw0tz2lyTvl53C7uHCcxvUyb4z2
                                6GwWEUqE85z8hUw8YVcpH3Jzj2Zt6vLosk4=
                                )
                        RRSIG NSEC 5 4 3600 20100209215255 (
                                20100110215255 24645 secure.chlab.net.
                                lDuL4dkXGqwgc2wyXgK1ZHcxlZP8kinFOYlZ
                                zLJSqNOK4JQrepVa2Y9db2agidFxS70sP8kj
                                THfgMd9yEVBqaF5HJ8TBMW3CFVg/u4htUONW
                                q2qznk5Jlmlhiy5TOin2AUmq8bS3w65SAeH5
                                UZDQqi4ms4JmsXejuygcq7pwDRAjud2Nvv+3
                                6PeJ3uW0Kw6M4oBkBEfZyNkfzTXRc8pHbPWu
                                TpuUATw/E1LMQYdTQLA2fCl7v9nWR5VJq4z1
                                hB4jPzrMSvNb1xm1TcE1rMr1crbnPUPrY/jn
                                EXwfTyAOEqiHmvr/aMwzsHThn35X14FMra0V
                                EWQUgbbgf1OSxcXQo3awB4NM9otCQWWlPjnp
                                gx9d99XWYIn/pkexXASlff1agk8yZULaCdYt
                                lfrsWsg3R7v/TiE3Q8FxYbWlyJVxCVqJNQ2S
                                mrRhXH7XaxxmvvJI7sklK+fuYNilFITTRvll
                                kYndOt5+MTvSTYK/rkHh+7PrJEGoTieN9zZd
```

Figure 13. Zone file for secure.chlab.net signed zone (16 KB), part 5 of 5.

```
secure.chlab.net.       3600  IN DNSKEY   257 3 5 (
                                AwEAAeu2+yxFHn/E8EAZN7lLJ7nrhWyPiurs
                                yuiHnxA8zyU55mGDM/yIHJ/dFNEzdsn2Ytp5
                                QQ3ysnEuUdR+OYkPnoISeY2ozHUjLg8m8Tfy
                                lXNvddMFW5Qunfogh+FNNQuHYsfpFjXM2eDt
                                cTVejCHikkREbEERbhcI+gJAVLu+PkBMnxyW
                                UyDME52AIY42HUcLAwBZZKg4MOB+pENIQBvB
                                GPthrTXGkleKcNxRGCRZDXlKgSPxf+voXfr8
                                deyBTQY13x03Tf1k+4nZYhANCFbw39MyfMHc
                                CmFHpUTq2G3QCxl1D6kMRflpxrDVgxIhmUYz
                                HKxGGuxoQuGQO3FB+21IIN5z3sZGJFKEkyxO
                                VoBqX4cn8GGUj6BmhwJhiwQhe+AjiZkGQb9G
                                GG9yroOjtKh8rJheCCC1oCGCZClIlXBXln10
                                ZTtO/UxKNckXEMQlglzrbL4X9nd3HlGviEZC
                                jlNuKQpCV0X+9MmKcDhK9/rseltz+ZsUW62U
                                3mJRx106eiXzhI/gt82s1V1ts4MasmYSapV7
                                eZOqC2vOB3E8G4ZC4lp4m6U3arJ1NqRGnC55
                                zzZv5PKa6sefX02YnSDguvG3a9nYAtGDj4Xz
                                /1AdXt3vMbjrfvtEM3gsB4ePJoUDN3TpvTW8
                                dZhNuzrLNuQyz7CNMGSdYE9xwNQcI7x89+mE
                                g2ad
                                ) ; key tag = 62944
```

Figure 14. Keyset for secure.chlab.net zone.

```
secure.chlab.net.       3600  IN DS 62944 5 1 (
                                476534EF4273D9BC63D37F41511BB369B03F
                                6A63 )
                        3600  DS    62944 5 2 (
                                D84278C232E5079EFEB8EFC49762697C3AA1
                                F27643648DCA62D4F05F0EB556DB )
```

Figure 15. DSset for secure.chlab.net zone.

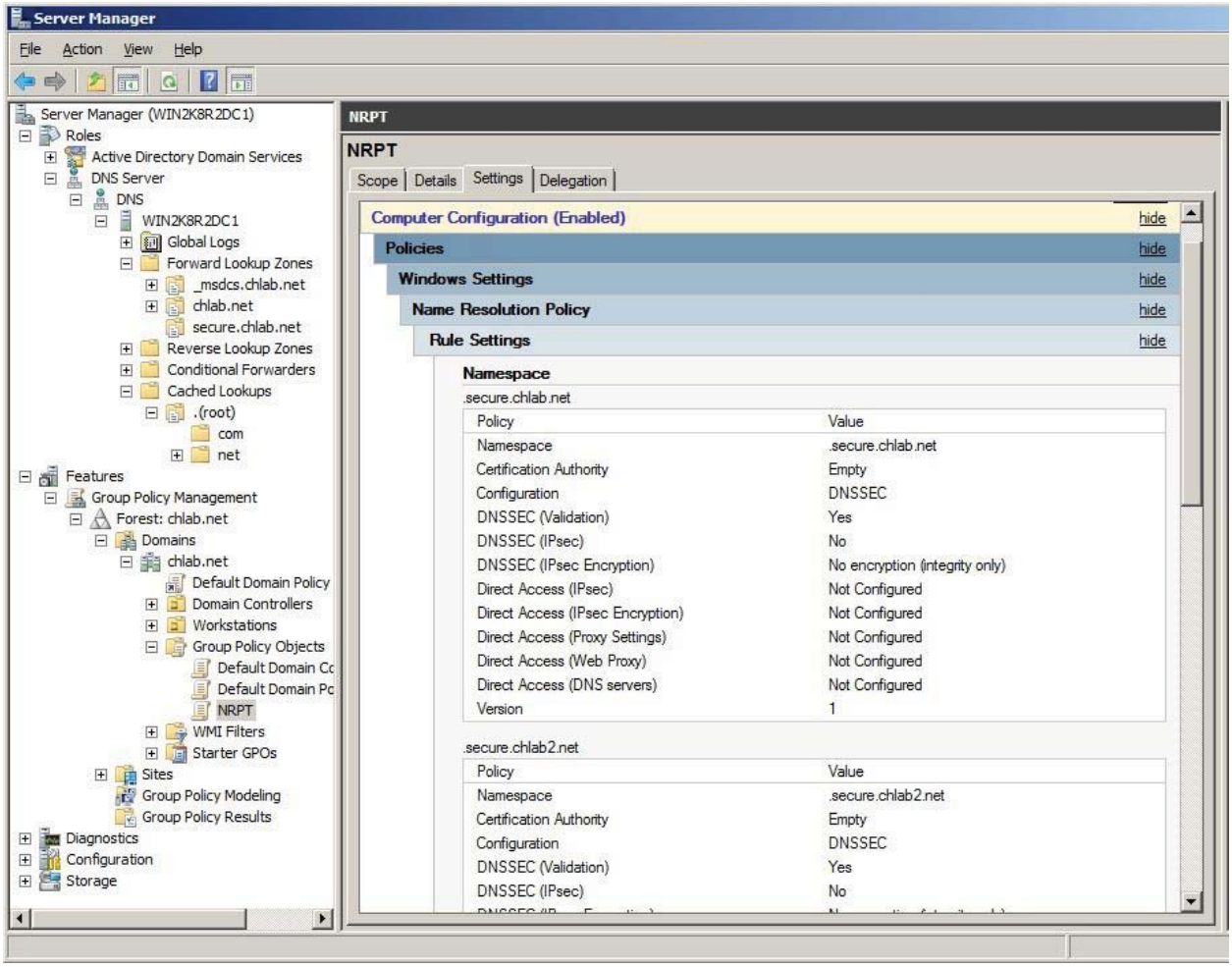

Figure 16. Screenshot of NRPT settings in Windows Server 2008 R2 management console.

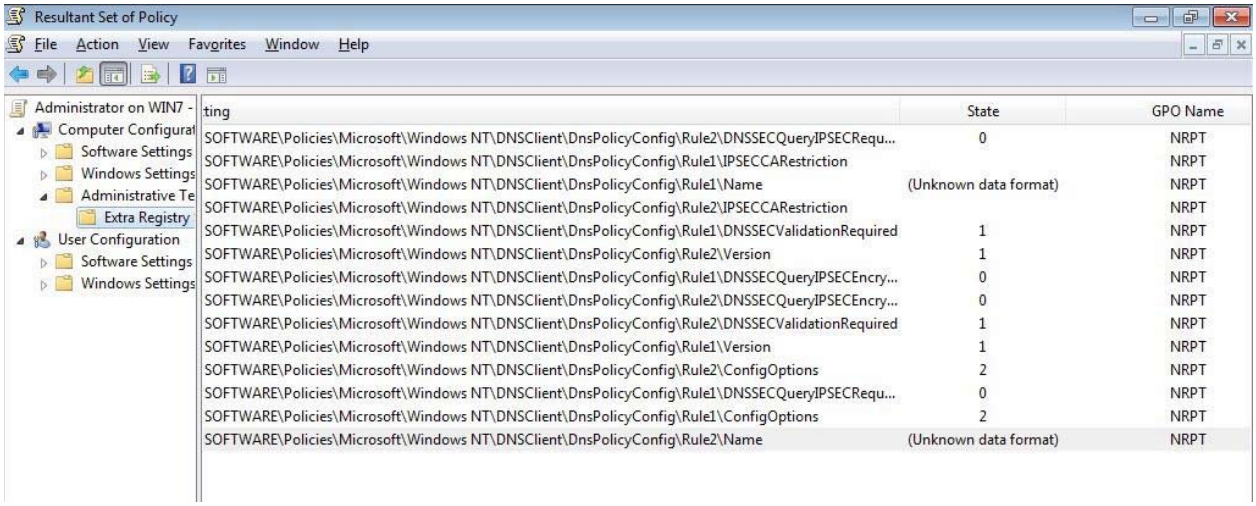

Figure 17. Screenshot of NRPT settings in Windows 7 resultant set of policy tool.

Appendix B – Test Plan

Test 1 – DNSSEC Functionality in Windows Server 2008 R2

i. Build a DNSSEC-enabled DNS server and a DNSSEC-signed zone, following the instructions in the Microsoft DNSSEC Deployment Guide. Document any discrepancies between actual install and the documentation.

ii. Issue a test DNS query from a Windows Server 2008 R2 DNSSEC-enabled caching server.

   a. On the caching server, verify

      i. The DNS Server cache is empty.

      ii. The caching server is configured to use the Windows Server 2008 R2 server hosting the signed zone as its forwarder.

      iii. The caching server is configured with the signed zone KSK in its trusted roots.

   b. From a command line on the DNS caching server, use nslookup <hostname> to issue the query.

   c. Is the response DNSSEC-validated? Use a packet capture tool to capture the query and response. Check whether the “validated” bit is set in the response.

iii. Issue a test DNS query from a Windows Server 2003 non-DNSSEC caching server. Is the non-DNSSEC server able to query the signed zone hosted in Windows?

   a. On the caching server, verify

      i. The DNS Server cache is empty.

ii. The caching server is configured to use the Windows Server 2008 R2 server hosting the signed zone as its forwarder.

b. From a command line on the DNS caching server, use nslookup <hostname> to issue the query.

c. Is the response DNSSEC-validated? Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

iv. Issue a test DNS query from a BIND DNSSEC-enabled caching server. Is the query DNSSEC-validated?

a. On the caching server, verify

i. The DNS Server cache is empty.

ii. The caching server is configured to use the Windows Server 2008 R2 server hosting the signed zone as its forwarder.

iii. The caching server is configured with the signed zone KSK in its trusted roots.

b. From a command line on the DNS caching server, use nslookup <hostname> to issue the query.

c. Is the response DNSSEC-validated? Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

v. Issue a test DNS query from a BIND non-DNSSEC caching server. Is the query successful?

a. On the caching server, verify

i. The DNS Server cache is empty.

ii. The caching server is configured to use the Windows Server 2008 R2 server hosting the signed zone as its forwarder.

b. From a command line on the DNS caching server, use nslookup <hostname> to issue the query.

c. Is the response DNSSEC-validated? Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

vi. Issue a test DNS query from a Windows Server 2008 R2 caching server against a BIND authoritative server with DNSSEC-signed zone. Is the query successful?

a. On the caching server, verify

i. The DNS Server cache is empty.

ii. The caching server is configured to use the BIND server hosting the signed zone as its forwarder.

b. From a command line on the DNS caching server, use nslookup <hostname> to issue the query.

c. Is the response DNSSEC-validated? Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

vii. Test DNSSEC Lookaside Validation.

a. Configure the Windows Server 2008 R2 DNS server Trusted Roots tab: Add a known DNSSEC Lookaside Validation server (Verisign?) to the Trusted Roots tab.

b. Issue a query against a signed zone that is known to be hosted at the DNSSEC Lookaside Validation service provider.

c. Is the query successful? Is the query DNSSEC-validated? Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

Test 2 – DNSSEC Functionality in Windows 7, Member of an Active Directory Domain

i. Build a Group Policy Object with a Name Resolution Policy Template (NRPT) that requires DNSSEC validation for the signed test zone. Apply the GPO to the Windows 7 client through the Active Directory domain. Run the RSOP.msc tool to verify that the Windows 7 client received the NRPT settings.

ii. Verify that the Windows 7 client has the Windows Server 2008 R2 DNS Server as its primary DNS server in TCP/IP configuration.

iii. Issue a DNS query from the Windows 7 client against the signed zone.

a. Type "ipconfig /flushdns" to verify that the local cache is clear.

b. Type "ping <hostname>" to trigger a DNS query for <hostname>.

c. Did the non-validating security-aware stub resolver successfully resolve the query?

d. Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

iv. Change the A record for <hostname> in the signed DNS zone, but do not re-sign the zone. (This should cause DNSSEC validation to fail.)

v. Issue a DNS query from the Windows 7 client against the signed zone.

a. Type "ipconfig /flushdns" to verify that the local cache is clear.

b. Type "ping <hostname>" to trigger a DNS query for <hostname>.

c. Did the non-validating security-aware stub resolver successfully resolve the query? If not, document any error messages.

d. Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

Test 3 – DNSSEC Functionality in Windows 7, Stand-alone Client

i. Follow the instructions in the Microsoft *DNSSEC Deployment Guide* to configure the Windows 7 client to require DNSSEC validation for the test zone. Verify that no Group Policy—NRPT is applying to the Windows 7 client.

ii. Issue a DNS query from the Windows 7 client against the signed zone.

a. Type "ipconfig /flushdns" to verify that the local cache is clear.

b. Type "ping <hostname>" to trigger a DNS query for <hostname>.

c. Did the non-validating security-aware stub resolver successfully resolve the query? If not, document any error messages.

d. Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

iii. Change the A record for <hostname> in the signed DNS zone, but do not re-sign the zone. (This should cause DNSSEC validation to fail.)

iv. Issue a DNS query from the Windows 7 client against the signed zone.

a. Type "ipconfig /flushdns" to verify that the local cache is clear.

b. Type "ping <hostname>" to trigger a DNS query for <hostname>.

c. Did the non-validating security-aware stub resolver successfully resolve the query? If not, document any error messages.

d. Use a packet capture tool to capture the query and response. Check whether the "validated" bit is set in the response.

Test 4 – DNSSEC Administration

i. Observe and document steps required for DNSSEC key management:
   a. Generating keys
   b. Key rollover
   c. Key distribution
   d. Look specifically for command line tools, right-click options, GUI interfaces, wizards, help files.
   e. Check to see if the DNS Server utilizes any existing Windows technologies to facilitate key management. For example, Windows Update, Certificate Management, Active Directory Replication.
   f. Does the DNS Server GUI provide any indications for what keys have been generated, what keys are associated with what zones, key lifetimes?

ii. Observe and document steps required for DNSSEC zone signing.
   a. Look specifically for command line tools, right-click options, GUI interfaces, wizards, help files.
   b. What steps are required to revert to an unsigned zone?
   c. Does the DNS Server GUI include any visual indications that the zone is signed?

iii. Make some mistakes intentionally, and observe whether the Windows DNS Server has any built-in safeguards to help prevent a system administrator from making the mistakes.
   a. Modify records in a signed zone (without re-signing the zone). Does DNS Server block this action or issue any warning to the DNS administrator telling the admin that it will be necessary to re-sign the zone?
   b. Generate a ZSK with an intentionally short life span and allow the key to expire.

i. Does the DNS Server GUI provide any visual indication that the zone has an expired key?

ii. Are any events logged in the DNS event log?

iii. Issue a query against the zone with the expired key. (Verify that the DNS query fails.) Does the DNS Server log an error in the event log?

iv. Is the Windows "nslookup" command line tool DNSSEC-aware?

a. Issue "nslookup <hostname>".

b. Observe whether the responses provide DNSSEC-related feedback.

c. Increase nslookup debug level to see more comprehensive information.

v. Are the Windows Event Logs DNSSEC-aware?

a. Look for DNSSEC messages in the DNS Server event log. Expected messages could include:

i. Zone signed (informational)

ii. Keys nearing expiration (warning)

iii. Keys expired (error)

b. Look for messages in the Windows 7 Application and System log.

i. DNSSEC validation failures

Test 5 – DNSSEC Documentation

i. Windows Server 2008 R2 documentation

a. Look in the OS help file for DNSSEC documentation.

b. Look in the DNS GUI help file for DNSSEC documentation.

c. Look at the DNS GUI and evaluate whether it is "self-documenting".

d. At a command line type “nslookup /?” and review the results for any references to DNSSEC.

ii. Windows 7 documentation

a. Look in the OS help file for DNSSEC references.

b. Look in the Internet Explorer help file for DNSSEC references.

iii. Microsoft Web Site documentation. What documentation exists at:

a. TechNet site

b. Support site

Appendix C – Glossary

ACL – Access Control List

BIND – Berkley Internet Name Daemon

DDoS – Distributed Denial of Service

DLV – DNSSEC Lookaside Validation

DNS – Domain Name System

DNSKEY – A new resource record type, containing the public encryption key

DNSSEC – DNS Security Extensions

DO – DNSSEC OK

DS – A new resource record type, Delegation Signer

EV – Extended Validation

GUI – graphical user interface

IETF – Internet Engineering Task Force

IP – Internet Protocol

IPSec – IP Security

KSK – Key Signing Key

MMC – Microsoft Management Console

MX – Mail Exchanger

NRPT – Name Resolution Policy Template

NSEC – A new resource record type, Next Secure

NSEC3 – A new resource record type, Next Secure version 3

R2 – Release 2

RFC – Request for Comment

RR – Resource Record

RRSIG – A new resource record type, Resource Record Signature

RSA – Rivest, Shamir and Adleman

SSL – Secure Sockets Layer

TCP/IP – Transmission Control Protocol / Internet Protocol

TLD – Top Level Domain

TTL – time to live

UI – user interface

ZSK – Zone Signing Key