2015

# Determining The Influence Of The Network Time Protocol (Ntp) On The Domain Name Service Security Extension (Dnssec) Protocol

Sherman J. Cold
*Indiana State University*

# VITA

Sherman J. Cold

## EDUCATION

| | |
|---|---|
| 2015 | Indiana State University, Terre Haute, Indiana<br>Ph. D. in Technology Management, Digital Communication Systems Specialization |
| 1990 | University of Nebraska—Lincoln, Lincoln, Nebraska<br>Master of Business Administration |
| 1984 | Brigham Young University, Provo, Utah<br>Physical Plant Administration |

## PROFESSIONAL EXPERIENCE

| | |
|---|---|
| 2001-Present | Utah Valley University, Orem, Utah<br>Associate Professor, Information Systems & Technology |
| 1996-2001 | Utah Valley University, Orem, Utah<br>Assistant Professor, Computer Science |
| 1994-1996 | Utah Valley University, Orem, Utah<br>Instructor, Computer Science |
| 1991-1994 | Utah Valley University, Orem, Utah<br>Network Administrator, Computer Science |

# DETERMINING THE INFLUENCE OF THE NETWORK TIME PROTOCOL (NTP) ON THE DOMAIN NAME SERVICE SECURITY EXTENSION (DNSSEC) PROTOCOL

---

A dissertation

Presented to

The College of Graduate and Professional Studies

College of Technology

Indiana State University

Terre Haute, Indiana

---

In Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

---

by

Sherman J. Cold

April 2015



Keywords: digital communications, technology management, DNSSEC, MiTM, Zone Signing Key, NTP, vulnerability





ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

COMMITTEE MEMBERS

Committee Chair: Dr. George Maughan

Professor, College of Technology

Indiana State University

Committee Member: Dr. David Border

Associate Professor, Electrical & Computer Engineering Technology

Bowling Green State University

Committee Member: Dr. Tijjani Mohammed

Associate Professor, Technology Systems

East Carolina University

## ABSTRACT

Recent hacking events against Sony Entertainment, Target, Home Depot, and bank Automated Teller Machines (ATMs) fosters a growing perception that the Internet is an insecure environment. While Internet Privacy Concerns (IPCs) continue to grow out of a general concern for personal privacy, the availability of inexpensive Internet-capable mobile devices increases the Internet of Things (IoT), a network of everyday items embedded with the ability to connect and exchange data.

Domain Name Services (DNS) has been integral part of the Internet for name resolution since the beginning. Domain Name Services has several documented vulnerabilities; for example, cache poisoning. The solution adopted by the Internet Engineering Task Force (IETF) to strengthen DNS is DNS Security Extensions (DNSSEC). DNS Security Extensions uses support for cryptographically signed name resolution responses. The cryptography used by DNSSEC is the Public Key Infrastructure (PKI).

Some researchers have suggested that the time stamp used in the public certificate of the name resolution response influences DNSSEC vulnerability to a Man-in-the-Middle (MiTM) attack. This quantitative study determined the efficacy of using the default relative Unix epoch time stamp versus an absolute time stamp provided by the Network Time Protocol (NTP). Both a two-proportion test and Fisher's exact test were used on a large sample size to show that there is a statistically significant better performance in security behavior when using NTP absolute time instead of the traditional relative Unix epoch time with DNSSEC.

# PREFACE

From the outset, the amount of attention given to server-side security for DNS name resolution seemed to be disproportionate to where the outcome really matters: the behavior of the Web client. This research specifically focused on the behavior of the Web client when the name resolution response had been intentionally hacked.

The process for this research evolved over time, necessitating the need to seek approval for a modified proposal. The researcher and his assistants struggled for two years with the original process before arriving at an approach that is presented here.

First efforts to cause a Man-in-the-Middle attack in a closed loop system designed for network experiments failed for two reasons. The first reason was the difficulty in establishing and keeping the designed network active long enough to gather data before Emulab detected an idle session and tore down the network. The second reason was the closed loop nature of Emulab that precluded participating in a bona-fide chain-of-trust for DNSSEC. Ultimately success in collecting data for this research came by establishing a DNSSEC server responsible for a registered domain, participating in a chain-of-trust for a Top Level Domain (TLD). Instead of trying to duplicate the process of a successful hack, the focus shifted on observing the influence of a successful hack under two different time stamp environments.

While it might seem like common sense to include in the DNS infrastructure, an absolute time stamp is not built-in default. This research tests the theory presented by several authors that DNSSEC is more secure when it uses an absolute time stamp.

# ACKNOWLEDGEMENTS

The father of Aikido, OSensei Morihei Ueshiba once said: "Failure is the key to success; each mistake teaches us something." I would like to thank the many teachers and helpers that encouraged me to keep going after each failure. I dedicate this research to all of the teachers I've ever had for their patience, kindness and personal sacrifices. Learning something new has got to be the most fun I've ever known.

I'd like to offer great appreciation to the members of my committee for their service, Dr. David Border (BGSU) and Dr. TJ Mohammed (ECU). A special thank you goes to my committee chairpersons from Indiana State University, Dr. Gerald Cockrell who started me down the right path, Dr. Ed Kinley who offered great technical inspiration, and Dr. George Maughan who offered kind guidance through to completion. Dr. Barry Lund (BYU) was also a great inspiration from the very beginning, only costing a burger from Burger Supreme in Orem.

I would be remiss if I didn't mention the persistent and timely advice from Mary "Mebby" Griffy, Program Assistant in the PhD program. I'd like to thank two former chairpersons: Dr. Chris Jones now at California State University, Northridge and Dr. Annette Gomm who are great examples of great scholars. Both of them saw something in me before I began a teaching career. I'd also like to thank a fellow graduate of the program, Dr. Jeff Daniels who always believed I would finish. Finally, I'd like to give special thanks to my wife Denise, someone who believed in me from the beginning and has always been my best friend.

TABLE OF CONTENTS

# LIST OF TABLES

LIST OF FIGURES

# CHAPTER 1

## INTRODUCTION AND CONTEXT OF PROBLEM

At the 2009 Black Hat Conference in Las Vegas, Nevada, Dan Kaminsky divulged a Domain Name Services (DNS) vulnerability and remarked that: "DNS is pretty much our only way to scale systems across organizational boundaries, and because it is insecure it's infecting everything else that uses DNS…" (Garretson, 2009)

DNS is vulnerable to cache poisoning, man-in-the-middle (MiTM) attacks, IP-spoofing for Dynamic DNS, and Distributed Denial-of-Service (DDOS) attacks, among others (Ariyapperuma & Mitchell, 2007).

### General Statement of the Overall Research

Traditional Domain Name Services (DNS) has been part of the Internet infrastructure since the start of the Internet. Every time emails are sent, a web pages are retrieved, or file are downloaded, a DNS servers are queried by an Internet clients to resolve the Internet Protocol (IP) addresses of the hosts. Unfortunately, no security is built into DNS (Atkins & Austeine, 2004).

While concerns are mounting about the security of DNS, because it is a major component of the Internet infrastructure, up to one billion land-based phones and two billion cellular phones are on the verge of being converted to Voice over IP (VoIP) technology (P. V. Mockapetris, 2006). Voice over Internet Protocol phones are also Internet clients and require DNS services to convert an assigned telephone numbers to IP addresses. Smart cellular phones can enable local

area wireless technology (Wi-Fi) VoIP in the presence of a Wi-Fi hotspots that provides connectivity to the Internet. VoIP phones can be targeted for eavesdropping without any changes to the network (Lin & Tsai, 2007).

**Why DNS Security Extensions**

Securing the infrastructure is so important that in December of 2006, the National Institute for Standards and Technology (NIST) issued publication 800-53r1: Recommended Security Controls for Federal Information Systems. This publication mandated the installation of a secure version of DNS--DNS Security Extensions (DNSSEC) protocol--in moderate and high impact systems of federal government Information Technology (IT) systems within one year (NIST, 2009b). "On March 26th, 2012, 910 unique Federal zones were signed and chained from the gov TLD, or 54% of all Federal zones" (Rose, 2012, p. 224).

Since Dan Kaminsky's disclosure of DNS vulnerabilities in 2008 (Kaminsky, 2008), DNSSEC deployment has continued world-wide resulting in the total number of signed-domains at more than 3.5 million (Rijswijk-Deij, Sperotto, & Pras, 2014). Figure 1 shows that out of 886 Top Level Domains (TLDs) available today, 707 or 79.8% are digitally signed by DNSSEC.

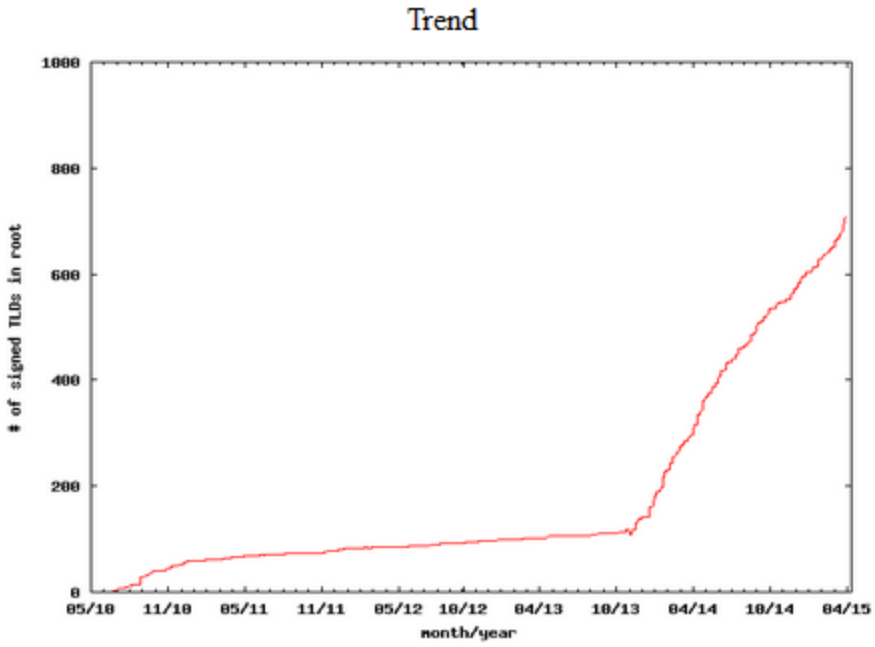


*Figure 1*. State of DNSSEC Deployment Worldwide. Since October 2013 the number of TLDs that are digitally signed from the 13 world-wide root servers has increased significantly to 79.8% (Lamb, 2015, para. 1).

The primary purpose for DNSSEC was to provide authentication and integrity for query responses received from the worldwide DNS database. Authentication and integrity is provided through public-key cryptography, which is the technique used to establish a public-key infrastructure (PKI). Keys in public-key cryptography (public-key cryptography is the technique used to establish a public-key infrastructure [PKI]) are used to generate signed certificates from the DNS servers providing responses to queries from Internet clients or other DNS servers (Ateniese & Mangard, 2001).

**DNSSEC Clients and Validation**

The purpose of DNSSEC was to provide a means to validate name resolution responses from the DNS worldwide database. DNSSEC clients should not accept a name resolution

response where the PKI signatures are not valid. To prevent attempts at PKI signature manipulation, some have argued that providing an absolute time stamp will enhance DNSSEC efficacy (A. Herzberg & Shulman, 2013; Osterweil, Massey, McPherson, & Zhang, 2014; Yih, Arsenault, & Sood, 2006).

Within a DNSSEC name resolution response there are Resource Records that contain the IP address of the intended web site. DNSSEC encrypts the Resource Record by signing the information creating a unique one-way hash. The hash is found in the Resource Record Signature (RRSIG) field of the name resolution response. The RRSIG Resource Record specifies a validity interval for the signature and uses an algorithm to identify the DNSKEY Resource Record containing the public key that a validator can use to verify the signature (Mantoro, Norhanipah, & Bidin, 2011). If any character in the hash is changed, the information should be rejected by the client as invalid because the signatures would not match.

A DNSSEC-enabled web site was set up and a specific DNSSEC client was used capable of validating each encrypted name resolution response. Each iteration involved manipulating the RRSIG hash to determine whether the DNSSEC client would accept and act on the name resolution response information. Enough iterations of the test were run to make the results statistically significant. Another set of iterations were run in the case where the DNSSEC server providing the name resolution used an absolute time stamp. A detailed description of the methodology used is found in Chapter 3.

## Relationship to Technology Management

The Internet of Everything is a term used to describe the acceptance of the integration of devices into the Internet (Bojanova, Hurlburt, & Voas, 2014; Massé, 2013). Because of the exponential growth of the Internet of Everything, end-user expectations are that the Internet will

be accessible and available all the time. It's not enough to have an Internet connection available, end users expect to be able to access the Internet to retrieve information at any time, and nearly everywhere. To meet this expectation, technology managers have to provide name resolution services that are secure (Schönwälder, Pras, & Martin-Flatin, 2003; Shirky, 2014).

Ever since the first Internet worm known as the Morris worm, security has had to be part of using the Internet (Berghel, 2001). Cyber attacks on US assets are increasing in frequency (Segal, 2013). Being able to establish secure sessions when communicating over the Internet is more important than ever. Technology managers need to make Internet client software available that is capable of properly validating name resolution responses. Without this capability, end users cannot be sure they are actually connecting to the legitimate, intended Internet resource.

## Background

DNSSEC was the solution adopted by the Internet Engineering Task Force (IETF), but it DNSSEC was not the only solution to secure DNS. For example, Daniel J. Bernstein created DNSCurve in 2009 (Bernstein, 2006) that uses an encryption algorithm called Elliptic Curve Cryptography (ECC), which is much faster than RSA (Edge, 2009). Additionally, there is a fundamental problem with managing and exchanging private keys securely in a network like the Internet. Additionally, research has shown that DNSSEC does not prevent all vulnerabilities, and in some cases, it does not function the way it should in every case from end to end.

## Review of Studies That Oppose the Project View

While no authors will argue against secure communications, not everyone agrees that DNSSEC is the protocol that should be used to provide that security. Kalafut & Gupta (2009) correctly point out that resolvers (DNS clients) in DNSSEC are only protected if the remote DNS server happens to deploy DNSSEC. The authors observed that host name to IP address

mappings rarely change and that "even when they change, the mappings stay within the same Autonomous System 97-99.8% of the time. These observations imply that any changes to a different Autonomous System (AS) should be scrutinized further" (p. 1). Kalafut & Gupta claim that resolvers should maintain a history of Autonomous System Numbers (ASNs) for each name resolution that can then be checked against the authoritative DNS server response or ASN whois database for accuracy. The advantage is that this technique can be implemented unilaterally within any security sensitive organization. Resolvers need not participate in DNSSEC to verify authenticity of name resolution authenticity.

Herberg and Shulman (2013) point out several flaws with DNSSEC beginning with the fact that if resolvers don't enforce validation, adopting DNSSEC may actually facilitate an attack by "providing long, fragmented [name resolution] responses" (p. 225). They claim that the often used 1024-bit RSA encryption used for signing zones is too weak. For example, DNSSEC does not prevent two attacks: fake subdomain injection and the name server pinning attack. The authors mention that when a resolver (DNS client) cannot establish a chain-of-trust from the root zone to the target domain, the resolvers default behavior is to not validate the response.

In their study of DNSSEC, Yong, XiaoChun, Gang, Zhen, and Yao (2012) found that the failure of the resolver to validate the response causes the recursive server (stub resolver) to continuously retry the query. This "will increase the load of the recursive server, and this vulnerability will be exploited to denial of service attacks" (p. 41). The authors note that while a forged DNSSEC response will not pass the validation check of the recursive server, the DNSSEC client will still not have the correct name resolution information.

## Review of Studies That Are Similar to This Project

Even though a DNSSEC server signs its zones and is part of a chain of hierarchically signed zones extending outward from the root zone, a compromised certificate could provide a hacker with the opportunity to spoof the DNS response (Cerf, 2014). The IETF is currently working on a project called DNS-Based Authentication of Named Entities (DANE) that attempts to mitigate this possibility by placing public keys (certificates) within the digitally signed zone file of the destination host name (RFC 7218). DANE is much like a business card not only providing information about who you are, but also proof that you are who you claim to be.

The challenge of PKI systems of reliably exchanging and verifying private keys among tens of thousands of service entities, is well-known. There have been many proposals that have attempted to address this challenge (Li et al., 2014; Massey, Mankin, Lewis, Russ, & Gudmundsson, 2001; Roman, 2011). Normally, Certificate Authorities (CA) have the responsibility for distributing and verifying certificates. The Unite-and-Conquer (UnC) system proposed by Karimi & Hauser does not use CAs to distribute certificates at all. Instead of binding certificates to entities (organizations, countries or companies), UnC binds certificates to Internet Protocol (IP) addresses. In a hierarchy separate from PKI, UnC distributes keys via a slightly modified version of DNSSEC that incorporates a customized version of the Secure Border Gateway Protocol (Karimi & Hauser, 2013).

For many years IP version 4 (IPv4) has been the address naming space protocol by default. However, the approximately 4.3 billion IPv4 addresses using a 32-bit address have all been assigned. IP version 6 (IPv6) uses a 128-bit address and was created to provide $7.9 \times 10^{28}$ more addresses than IPv4. Because IPv6 addresses are 128 bits, IPv6 addresses are rarely manually assigned. Typically IPv6 addresses are automatically generated through the Neighbor

Discovery Protocol (NDP) in both stateful and stateless autoconfiguration. The stateless autoconfiguration uses the StateLess Address AutoConfiguration (SLAAC) mechanism which is new to IPv6, but non-existent in IPv4. SLAAC does not work with DNSSEC. To solve this situation, Rafiee & Meinel propose an asymmetric cryptography to establish a trust relationship with the DNS server. The authors want to extend the RDATA field within the Transaction Signature (TSIG) protocol used in DNSSEC that they call the CGA-TSIG (Rafiee & Meinel, 2013).

The foundation for Internet Privacy Concerns (IPCs) is the general premise of privacy itself. Involved in the general sentiment of privacy is a fundamental belief in human dignity. One of the first court cases to establish a precedent for human dignity was a famous case that came before the Michigan Supreme Court in 1881. In this case a woman filed a complaint against a man who had been present during the delivery of her child. It was presumed that the man was a doctor because the social norm at that time was that a doctor would be the only man present during a delivery *DeMay v. Roberts* (1881). The fact was that the man was not even in the medical profession. The court ruled that the man had violated the woman's privacy (Bruin, 2010). Even though there was no specific law that guaranteed the woman's privacy, social norms required it. Likewise, even though there are few laws that guarantee the privacy of information on the Internet, the expectation exists that our information should be private as a matter of human dignity.

## Philosophy

A significant amount of scholarly activity surrounds the very definition of privacy. Within the realm of privacy theory, many have defined privacy contextually, looking at privacy norms within the bounds of relationships, situations, or context. Martin (2012) explains that:

"individuals are privacy pragmatists who exchange information for specific benefits, i.e., better relationships, power, team cohesion, etc., and these exchanges carry forth actual and hypothetical social contracts" (p. 520).

**Social Contract Theory**

Fried (1968), Rachels (1975), Inness (1992), and later Cohen (2002) take privacy social contract theory a step further by claiming that relationships require privacy as a necessary condition for a human relationships' existence. A normal part of human relationships requires the mutual giving of gifts in the form of information. The gift only has value when people have secure possession of the information they want to provide, usually private information (Bruin, 2010). Others see the privacy social contract as contextual, varying by situation, regardless of the individuals involved. Moor combines the two viewpoints by claiming that privacy can be attached to a situation and individuals can have varying levels of access to private information regarding that situation (Moor, 1997).

**Contextual Integrity**

In similar fashion, privacy can be viewed as contextual integrity. Nissenbaum (2004, 2009) sees privacy as the negotiated agreements about how information is accessed and distributed. Margulis agrees by saying that privacy represents control over transactions between people. The ultimate aim of this control is to enhance economy or minimize individual vulnerability (Margulis, 2003). Margulis is quick to point out that this control has limits on access to information about self, groups, and even large collectives. This idea is particularly important considering that privacy allows people to discuss political expression and criticism. Privacy allows non-political freedom of association in family and religion. Privacy provides opportunities for self-assessment and experimentation (Westin, 1967).

**Human Dignity**

The first court case mentioned in this discussion was *DeMay v. Roberts* (1881) where privacy was defined by the court within the bounds of human dignity. In *Haynes v. Alfred A. Knopf Inc.* (1993), Judge Richard Posner set a standard for the privacy of human dignity when he ruled that the mysteries of privacy universally extend to the intimacies of the bedroom and the bathroom (Allen, 2013). Allen endeavors to build on Nissenbaum's description of information privacy by saying that there are ethical norms of appropriateness that are standards located above ordinary guidelines of taste and tact.

Avishai Margalit (2001) claims that a decent society embraces two related ideas: one idea is the concept of the non-humiliating society. This is a society whose institutions do not humiliate those who do are dependent on them. The other concept is the civilized society where members do not humiliate each other. An invasion of privacy is humiliating both by humiliating invasion by institutions and humiliating invasion by individuals.

**Autonomy**

If one assumes that the possession of correct beliefs about what others know about an individual fosters one's autonomy, then it's in the individual's interests to be in control of what is known about them (Bruin, 2010). This idea is justification for the protection of confidentiality. Doyal clearly links the protection of confidentiality to a protection of a patient's right to protect their personal information and claims that this kind of personal information is worthy of the most stringent protection (1997).

Encouraged by Warren's hatred of the invasion of social privacy at the time, Louis Brandeis co-authored an article in the Harvard Law Review on The Right to Privacy in 1890 that considered if law could protect the rights of privacy of the individual (Keefe, 1980; Post, 1991;

Warren & Brandeis, 1890). This famous article evaluated the current law against defamation regarding slander and libel to see if either tort could protect privacy. The conclusion was that defamation only protected an individual's reputation, not their privacy. The authors claimed that the loss of privacy was damnum absque injuria (a loss that comes from something other than a wrongful act for which there is no current legal remedy.)

William Prosser's review of the Warren and Brandeis' legal opinion regarding privacy had a powerful influence on the framework of American law (Citron, 2010; Schwartz & Peifer, 2010). Prosser proposed four legal torts that granted protection against certain kinds of invasive behavior. State courts and legislatures adopted this framework that acknowledged the significance of permitting each person to use self-determination when forming their life. Court attempts to protect privacy have evolved as a balance between an individual's right to privacy and First Amendment rights.

In 2001 a memoir was published by a lady named Kaysen called The Camera My Mother Gave Me. The book led to a court case *Bonome v. Kaysen* (2004) whereby Bonome sought legal relief from the negative things Kaysen disclosed about him as her ex-boyfriend. Ultimately, the First Amendment made all the difference in the case. The court identified a rather equal balance between Kaysen's right to tell her own story and Bonome's right to control the sharing of information about his private life (Schwartz & Peifer, 2010).

## Moral Viewpoint

Many defenders of a privacy doctrine believe that specific claims to privacy are found in a moral principle. Although there are times when these moral arguments are made explicitly, more often than not such moral claims are implicit. "Claims that privacy rights are rooted in

ideals of autonomy, personhood, intimate association, self-hood, or human dignity all seem to reflect the belief that the favored values are morally appealing" (Rappaport, 2001, p. 2).

A contrary viewpoint is that the moral approach is completely wrong. This approach believes that a court should never look to the moral principle to decide any scope of privacy rights. Posner believed that there will exist a persistent controversy over any underlying moral questions about privacy (1978). Not only would questions regarding the greater human good be controversial, but would also be ultimately unsolvable.

A middle ground seems to be that scholars should attempt to clarify how moral principles define the specific scope and structure of privacy rights. This approach favors some moral principle without attempting to prove that same principle. For example, one cannot prove that homosexuality is morally right or wrong. However in order to structure how privacy should be structured, a privacy jurisprudence can be created that guides how privacy should be defined.

**A Right to Privacy**

Corlett (2002) writes that a moral right to privacy falls within the realm of a right to liberty. Privacy is part of a rights package which includes the moral right to self-rule and the freedom of expression. Legally speaking, the scope of the legal right to privacy includes personal decisions about an individual's life. The right to privacy is often based on the contents of the Fourth and Ninth amendments to the Constitution and is found in the legal concept of an ordered liberty. Ordered liberty determines what freedoms can be limited by the need for order in society. Corlett also makes the point that the right to privacy is alienable. A person can give up their right to privacy, making this right discretionary. For example an employee can refuse to give more information to an employer about themselves than legally required, but may also choose to provide that information for the good of the organization.

Bedi (2005) claims that any constitutional commitment to privacy is not only problematic but unnecessary. In *Lawrence v. Texas* (2003), the court laid the groundwork for rendering the right to privacy obsolete. This Supreme Court decision overturned a previous Texas anti-sodomy law. Bedi postures that scholars have failed to realize that the repudiation of morals legislation renders the due process right to privacy obsolete.

## Internet Privacy Concerns

A significant portion of IPC involves maintaining privacy when conducting financial transactions. Identity theft, bogus websites, and phishing email, are all common tools used by thieves for financial gain. Uusitalo, Catot & Loureiro (2009) note that when attempting to secure private information, "[t]he cost of the method typically grows the more secure the method. Also, the more secure methods tend to be more complex toward the user" (p. 168).

IPC threats not only threaten financial transactions, but many transactions found in both the public and private sector in cyberspace. Cyberspace has become the nervous system of the economy, no longer a luxury-- but an integral part of the whole. "The healthy functioning of cyberspace is essential to our economy and our national security" (National Strategy to Secure Cyberspace, 2003, p. vii).

There is a growing perception that the Internet is an insecure environment. However the availability of ever inexpensive computers and other Internet – capable mobile devices, has made Internet vulnerability greater than ever. Typically end-users have poor practices when it comes to protecting their Internet devices (Fang, 2007). Additionally, work by Georgiev, et al. (2012) suggests that the Secure Socket Layer (SSL) protocol used to encrypt private information over the Internet is not secure. SSL uses PKI cryptography, the same PKI used for DNSSEC to accomplish its encryption.

The way in which signed certificates are evaluated for acceptance between DNSSEC servers and the Internet clients they serve, is based on a relative time stamp: the current time relative from the UNIX epoch: January 1, 1970. DNSSEC does not have an internal time clock built into its protocol.

The Network Time Protocol (NTP) is a Free and Open Source software (FOSS) time-keeping solution that provides an absolute time reference to a computer network (NTP Project R&D, n.d.). NTP has a network hierarchy similar to DNS and can be run jointly with DNSSEC to provide an absolute time stamp to the signature and inception fields of the Resource Record Signature (RRSIG) of DNSSEC.

## Problem Statement

Although DNSSEC is a promising solution to the problems suffered by legacy DNS, its certificates providing authenticity and integrity can be forged (Basu & Muylle, 2003; Dijk, Rhodes, Sarmenta, & Devadas, 2007; Wu & Zhou, 2011). The number of signed-DNS domains is increasing world-wide to provide secure name resolution for all Internet use. By intercepting name resolution traffic, a hacker can successfully issue a MiTM attack because of DNSSEC's default relative time. By using an absolute time stamp DNSSEC will be more secure by making it harder to create a MiTM attack. DNSSEC clients should be able to validate that name resolution responses are bona fide. Therefore, the problem this research investigated was whether using NTP affects DNSSEC client security performance.

## Research Purpose

The purpose of this research was to evaluate a DNSSEC client's ability to validate a name resolution response and determine the significance of using NTP to improve the ability to

detect attacks on DNSSEC certificate authentication and verification when an absolute time stamp was used.

## Need For The Research

While several research projects have evaluated the effectiveness of DNSSEC on the server side, research on the client side of DNSSEC was not found. A review of the literature showed that there are several concerns about implementing DNSSEC to provide the level of security expected from DNSSEC. While DNSSEC does enhance name resolution communication channels, other issues were not addressed in Request for Comment 2065 (DNSSEC) and Request for Comment 2535 (DNSSEC) (Eastlake, 1999; Eastlake & Laufman, 1997). Many authors have written about one problem relating to using a Public Key Infrastructure (PKI) in domain name resolution, that of managing the private keys (Ahmad, 2008; Cagalaban & Kim, 2011; B. M. Chen, Chen, & Chen, 2011). Few authors have written about the need for an absolute time stamp to prevent replay attacks when using PKI. This research was needed to add to the body of knowledge regarding the implementation of DNSSEC in particular, and securing the Internet infrastructure as a whole.

While some recommendations have been made in the literature concerning PKI, little research appeared to have been done on DNSSEC itself. The proposed research tested a hypothesis about the efficacy of DNSSEC validation on the client side. This research also tested a hypothesis on using NTP to improve DNSSEC's ability to detect a corrupted hash in the server response. Success was defined as the null hypothesis being rejected with a statistical significance, where $p \leq 0.05$.

$H_0$: There is no difference between using a relative time stamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

$H_a$: There is a difference between using a relative time stamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

## Assumptions

DNSSEC uses public-key cryptography certificates for authentication and verification. Other services that use public-key cryptography certificates for authentication and verification have a documented vulnerability as a direct result of the time stamp used in the certificate known as a replay attack. The assumption is that DNSSEC also experiences the same defined vulnerability.

For each iteration of testing, only the researcher validated the data through the use of a tally sheet, keeping track of each public certificate hash change and the results of the experiment.

It is assumed that it is possible using documented cracking techniques to alter the RRSIG hash, corrupting the signature that will alter the certificate. The DNSSEC client should not be able to validate the authentic response as valid.

## Limitations

In its experiments, NIST used a 20+ node Emulab to test its implementation of DNSSEC. NIST procedures for setting up DNSSEC are outlined in Standard Publication (SP) 800-81. For this research a single Virtual Private Server (VPS) was used with a single DNSSEC client. GoDaddy.com hosted the Internet-accessible VPS. The performance of the VPS provides the ability to reproduce the research for any digitally-signed domain participating in a chain-of-trust for any TLD.

Confidence limits are expressed in terms of a confidence coefficient. Even though the choice of a confidence coefficient can be arbitrary, in practice 90 %, 95 %, and 99 % intervals are often used, with 95 % being a common choice (Snedecor & Cochran, 1989). The choice of a

95% confidence coefficient means that the proportion of samples may be expected to include the true mean. There is a possibility that a 95% confidence interval will not include the true mean of the population, however the sample size selected is more than twice the sample size calculated to adequately represent the population.

This research used the default DNSSEC 1024 bit RSA ZSK and 2048 RSA KSK cryptography as defined by SP 800-81 that encrypts the communication between a DNSSEC client and a DNSSEC server acting as a stub resolver and the higher level encryption used along the DNSSEC hierarchy--between DNSSEC root servers and Start of Authority (SOA) servers. In all cases, the test involved in this research attempted to spoof the certificate exchange between participates in order to successfully change the legitimate response from a DNSSEC query. Although there are no root DNSSEC servers in this study, the 2048 RSA KSK encryption that will be tested is the same encryption used by root DNSSEC servers.

## Methodology

This research established two groups of three nodes on an RFC 1918 private virtual network provided by the University of Utah Emulab (White et al., 2002). The first group implemented DNSSEC as is, using relative time stamps. The second group used the NTP daemon to provide an absolute time stamp from a stratum 1 United States Naval Observatory (USNO) time server for the U.S. Mountain Time Zone out of Colorado Springs, CO (USNO NTP Network Time Servers, n.d.).

A node in each group used a DNSSEC server implementing the Berkley Internet Naming Daemon (BIND) version 9. Each group established two DNS zones: a parent zone and a child zone. Each group had one workstation running Ubuntu 10.10 Desktop as an Internet client capable of running Mozilla Firefox 3.6.2. The child zone DNSSEC server acted act as the stub

resolver for the workstation acting as an Internet client. An attempt was made to manipulate the certificate on the query response simulating an attack against response certificate from the parent zone DNSSEC server. The private network was setup so that only the parent zone will be able to resolve the hostname lookup. After each attempt, a script flushed the cache of the child zone DNSSEC server so that no lookups are served from the stub resolver cache. Data was gathered in a yes/no fashion, indicating whether the DNSSEC client still validated the server response once the response certificate was changed. Each group was tested for validated through 385 attempts to gather enough data.

## Terminology

Cache Poisoning- DNS cache poisoning consists of changing or adding records in the resolver caches, either on the client or the server, so that a DNS query for a domain returns an IP address for an attacker's domain instead of the intended domain (Olzak, 2006).

Cracking-The act of intentionally breaching computer security, often on a network, with the malicious intention of causing harm or damage (Raymond, 1996).

DNS – Domain Name Services – A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.

DNSSEC – Domain Name Security Extensions - DNSSEC extensions to the DNS protocol that provide a layer of authorization between requesting clients and DNS servers. The extensions provide a way for clients to check the authenticity of a response to protect against both poisoning and other redirection methods used in man-in-the-middle and phishing attacks (Cubrilovic, 2008).

IP Spoofing- A technique used to gain unauthorized access to computers where the intruder sends messages to a computer with an IP address indicating that the message is coming

from a trusted host. The receiving computer accepts the message as authentic (IP Spoofing, 2008).

Root Key Rollover-A planned practice within cryptographic key distribution systems where the key used to sign subordinate zones is periodically changed to increase cryptographic security (Michaelson, 2010).

VoIP-Voice over IP- VoIP involves sending phone conversations in digital packets instead of using the traditional committed circuits of the public switched telephone network. A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by common telephone service (Definition - What is VoIP?, 2008).

# CHAPTER 2

## REVIEW OF THE LITERATURE

### Privacy in the United States

The foundation of a Western notion of privacy began with an attempt at a legal definition of privacy in 1890 by Samuel Warren. Warren hated the blatant invasion of social privacy in his day. He and Louis Brandeis co-authored a renowned essay The Right to Privacy that appeared in The Harvard Law Review. This article considered whether the current law could protect the rights of privacy of the individual; the "right to be left alone" (Keefe, 1980; Post, 1991; Warren & Brandeis, 1890). The Right to Privacy compared the 1890 law against defamation in regards to slander and libel to evaluate if those legal torts could protect individual privacy (Kasper, 2005).

Previously, the legal view was that privacy protection was limited to the bounds of the physical borders of body and property. Jacobs (1995) explains how Brandeis felt that privacy protection should extend beyond individual possessions.

> Brandeis was a relentless critic of outsized institutions, whether they were industrial monopolies or the bureaucratic state that dwarfed the individual and demeaned the citizen. 'He has so much respect for private property,' wrote Max Lerner, 'that he wishes it were more equitably distributed, so much respect for

> capital that he wishes it to flow freely instead of being concentrated in a money trust (Jacobs, 1995, p. 62).

*Olmstead v. U.S.* (1927) was a Supreme Court case where the court reviewed if the use of private telephone conversations that had been wiretapped were admissible into evidence. The defense argued that the act constituted a violation of the defendant's Fourth and Fifth Amendment rights in the Constitution (Steiker, Fall 2009). The defense lost the appeal 5-4. In response, Brandeis states:

> The makers of our Constitution ... knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things.... They conferred, as against the Government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use of evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth (Brandeis & Strum, 1995, p. 206).

Warren and Brandeis claimed that the loss of privacy was *damnum absque injuria* (a loss that comes from something other than a wrongful act for which there is no current legal remedy.)

Legal scholars in the late 19th century often used Blackstone's formulations to support suppression of the press. Supreme Court Justice Joseph Story said that "press freedom could be used but not abused" (Smith, 2008, p. 81). However new the limited protections of privacy were, going to court for injunctive relief could be problematic. Plaintiffs risked exposing even

more private information on the stand. Presidential candidate Grover Cleveland was advised to sue over published stories about his sexual escapades, but the fear of an even great expose' into his private life held him back. Warren and Brandeis (1890) offered a legal perspective on the boundaries between a person's public and private life. They argued that tort law should protect the privacy of the individual from the press, the photographer, or any other modern device used for reproducing scenes or sounds (Citron, 2010).

During Warren and Brandeis' time, protecting privacy had more to do keeping your social status by keeping personal affairs personal. Bezanson explains how the purpose behind protecting privacy has changed since The Right to Privacy was first published: "In 1890, privacy was rooted in rural values, representing an effort to maintain social organizations and values that were threatened by urbanization. Today, however, privacy is rooted in values of individualism" (Bezanson, 1992, p. 1135).

**Prosser's Influence on Privacy Law**

Like Warren and Brandeis, William Prosser's article on Privacy published in 1960 had a significant effect on the canon of American law. Prosser was concerned that there was still lacking a set of torts protecting individual privacy. Prosser writes (1960) that the Court of Appeals of New York rejected the appeal in *Roberson v. Rochester Folding Box Co.* (1902) in which the defendant had used a picture of a pretty young lady to advertise flour without her consent. The Court of Appeals declared that "the right privacy did not exist, and that the plaintiff was entitled to no protection whatever against such conduct" (p. 385).

To counter the lack of protection of privacy, Prosser created four privacy torts "providing just enough theory, doctrine, and rules of thumb to create a level of comfort for American judges deciding cases and for state legislatures enacting tort privacy statutes" (Schwartz & Peifer, 2010,

p. 1929). The torts that Prosser framed even today allow a plaintiff to file a civil suit to recover from damages by a defendant for:

1. Intrusion into private affairs.
2. Disclosing publicly facts that are deemed embarrassing and private.
3. Placing a person in a false, negative view in the eye of the public.
4. Misappropriation of a name or a likeness (Citron, 2010).

An example of how Prosser's privacy torts are used is found in the *Bonome v. Kaysen* (2004) case. In 1993 J. Joseph Bonome, the owner of a landscape business had an extramarital affair with Susanna Kaysen. That same year Kaysen had published a memoir called Girl, Interrupted which was later made into a 1999 movie. Bonome and Kaysen's affair ended in 1998. Kaysen then wrote a new memoir in 2001 called The Camera My Mother Gave Me in which Kaysen portrays the boyfriend in a very negative light. Bonome filed suit against Kaysen claiming an invasion of privacy. Prosser's privacy torts guided the courts to find for Kaysen without even a trial.

> The First Amendment made all the difference in the outcome of the case. At the nonconstitutional level, the court had identified a fairly equal match between Kaysen's right to disclose her life story and Bonome's own interest in controlling 'the dissemination of private information about himself" (Schwartz & Peifer, 2010, p. 1931).

## Social Contract Theory of Privacy

Several scholars believe that privacy should always be defined in context. Meaning that privacy norms are defined in relationships or situations. A contextual view of privacy evaluates

privacy expectations as being negotiated within a "community or situation" (Martin, 2012, p. 520). For example, individuals exchange information (giving up absolute privacy) in order to gain benefits like information, better relationships, power, status within a group, etc. These information exchanges establish actual and virtual social contracts.

> Fair information practices, therefore, mediate privacy concerns raised by disclosure and subsequent use of personal information by empowering the individual with control and voice, even if people do not choose to invoke the procedures (Culnan & Bies, 2003, p. 330).

**Contextual Integrity in Social Contract Theory**

Nissenbaum believes that any social contract involves privacy as contextual integrity. This theory regards social contracts as negotiated agreements about how the information shared will be accessed and distributed (1997, 2004, 2011). Information gathering and sharing should always be appropriate to the context of the situation or relationship. In other words, the privacy expectations within a social contract can vary depending on the situation. Also noteworthy is that these situational privacy expectations take precedence over universally defined privacy norms.

Moor goes farther to suggest that not only can the level of privacy vary by situation, but that within those situations different people may be given different levels of access to private information at different times (1997). He contends that privacy can have both an instrumental value and an intrinsic value. Privacy has an instrumental value because it protects us from harm. But privacy also has intrinsic value because it allows us to form bonds with other people that might be difficult to form in public. In his article *Why is privacy important?* James Rachaels

(1975) contends that the ability to vary the amount of privacy given to private information allows us to form varied relationships with other people. Deborah Johnson in her book *Computer Ethics* claims that privacy not only has an intrinsic value, but is an essential element to human autonomy (Johnson & Miller, 2009).

Stephen Margulis (2003) appears to agree with Johnson when he says: "Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (p. 245). Margulis bases his understanding on Altman's theory of privacy in which privacy's purpose is to regulate levels of social interaction between people (Altman, 1977) and Westin's book *Privacy and freedom* (1967) where the author maintains that privacy affords people "the opportunities of self-assessment and experimentation" (Margulis, 2003, p. 246). Margulis admits that both of these foundational theories are limited in their approach, meaning that they only address how individuals or individuals within groups control information access to themselves within a social contract. He also admits that attempts to regulate different levels of privacy may at sometimes be unsuccessful. The results of which may be more or less privacy than originally intended.

**Human Dignity as a Justification for Privacy**

Some invasions of privacy are contrary to human dignity. One of the first legal cases involving human dignity was the *DeMay v. Roberts* (1881) where the plaintiff filed a complaint against a man Scattergood who remained present during the delivery of her child. In all fairness, Scattergood was a friend of the doctor and was asked to help hold down the patient. However, the act was such an affront to the social norm at the time that it was presumed that the defendant was in the medical profession when in fact he was not (Bruin, 2010). Chief Justice Marston of the Michigan Supreme Court rejected the claim that Mrs. Roberts consented to Scattergood's

presence because she had held his hand during delivery. Even though this case was written nearly a decade before the Warren and Brandeis article (1890), neither they nor Prosser (1960) ever mentioned human dignity as a justification for privacy (Bernabe, 2012).

Much of the concept of privacy benefiting human dignity revolves around the concept of informed consent. The modern concept of informed consent was established in 1914 when Justice Cardozo in *Schloendorff v. Society of New York Hospital* (1914) said: "every human being of adult years and sound mind has a right to determine what shall be done with his own body" (Samz, 2007, p. 3).

Human dignity can be manifested as informed consent. Informed consent goes beyond the ramifications for medical procedures as Alan Kato Ku (2005) writes. Many cell phones today have cameras built-in. On December 1, 2003 a Washington state resident Jack Le Vu was the first person charged in the United States for taking upskirt photos. Washington had borrowed a voyeurism law from California, but in this case the law did not extend to public places. The court ruled that even though the act occurred in public, the victim had a reasonable expectation of privacy (Kato Ku, 2005).

What is a reasonable expectation of privacy in public has changed considerably with public surveillance using video cameras. Public surveillance is unregulated for the most part and "beyond the scope of the Fourth Amendment" (Capers, 2013, p. 960). While some believe public surveillance infringes upon privacy and anonymity, others believe surveillance cameras aide in fighting crime. Slobogin (2013) argues that members of the public could have seen what surveillance technology sees, therefore there is no invasion of privacy. In 2012 New York City announced its partnership with Microsoft Corporation to implement the Domain Awareness System that analyzes information from about 3,000 surveillance cameras. The Domain

Awareness System allows police to scan license plates, measure radiation levels, cross-check databases, etc. (Long, 2013).

In Oakland, California the city has built a combined Data Awareness Center (DAC) for law enforcement data for the city and the port. However, the DAC has become politically uncomfortable since the National Security Agency (NSA) revelations on domestic spying. Despite passing up the possibility of Homeland Security funding, the Oakland City Council is delaying expanding the DAC (Mosher et al., 2014). Face recognition technology can now analyze video feeds in real time, looking for suspicious activity. People exchanging objects, person identification, vehicle counting, and human activity prediction are all capabilities being built into surveillance systems (Gowsikhaa, Manjunath, & Abirami, 2012).

What are the issues when such surveillance technologies are not used in public, but at work? Botan (1996) writes that surveillance at work should be a common expectation. "The primary characteristic of a surveillance society is the use of various technologies and procedures directed toward both economic and personal life" (p. 294). D'Urso (2006) points out that surveillance for general workplace monitoring might be appropriate until it is done to identify workplace wrongdoing. Monitoring web site activity and email communication of workers is a common practice.

Workplace email in and of itself is problematic when it comes to privacy expectations. Kurman (2014) suggests that "supervisors must avoid intemperate and inflammatory email comments about employees when communicating with other managerial representatives" (p. 12). The 2014 Sony data breach exposed sensitive employee information and embarrassing emails of upper management ("Lawsuits against Sony Pictures", 2014; "Massive Cyber Breach at Sony", 2014). Privacy expectations in an era when The Internet of Things (IoT) is so prevalent, brings

up Internet Privacy Concerns (IPCs) as maintaining personal privacy continues to be an evolving challenge.

## Autonomy Permitted by Privacy

Johnson's view that privacy is an essential element to human autonomy has a broader scope than social contract theory. Autonomy as defined by privacy scholars includes patient confidentiality. Work by the academic lawyer Ian Kennedy deemed *bioethics*, was a primary factor in the British movement for audit and consumer choice in medicine in the 1980s (Keown, 2012). Kennedy called bioethics an important part of the audit society that demands legitimacy for autonomy in patient decision making (Wilson, 2012). This includes end-of-life issues and the evaluation of human life (Keown, 2012). Doyal (1997) cites Jean McHale's book *Health Care Law* (McHale & Fox, 1996) when he quotes: "The right to privacy relates to the right of the individual to control access to his own personal information ... [and] ... applies to all personal information ... It is confidential information which is especially worthy of protection" (p. 25).

Privacy as an element of autonomy has been described by Schwartz as a unitary concept in Germany or a limited group of torts in the United States (Schwartz & Peifer, 2010). Autonomy and privacy vary even among five European countries where a nursing study was done on the differences among the elderly (Leino-Kilpi et al., 2003). In the *Bonome v. Kaysen* (2004) case mentioned earlier, the plaintiff lost the case and the book was allowed to be published. In Germany, there was a similar case where Maxim Biller's novel *Esra* included characters too close to real people in a relationship with the author. In a 5-3 majority decision the German high court ruled novel intruded into the private sphere of the real-life person on which the character of Esra was based (Taberner, 2006; Top German court confirms ban, 2007). In this case, the plaintiff won and *Esra* was never published.

## Moral Aspect of Privacy

A difficulty for defenders of privacy rights is that there is nothing in the text of the Constitution, in its intent, or in American tradition that establishes a right to privacy. Rappaport (2001) offers a moral quandary when he says:

> None of these standard modes of constitutional interpretation can explain why privacy rights extend to abortion but not homosexual relations, to contraception but not adultery, to the withdrawal of life support systems, but not to assisted suicide. How, if at all, can these distinctions be justified? (p. 2)

The answer to Rappaport's query is provided by defenders of privacy rights through a moral principle. David A.J. Richards is a well-known defender of the moral principle. His book *Toleration and the Constitution* (1989) supports a contractarian theory of interpretation of the Constitution- - a theory that supports a moral sovereignty of the people. Richards affirms that toleration and or respect for conscience and individual freedom is a central constitutional ideal.

The moral principle approach is referred to as Kantian in nature. Immanuel Kant was a German philosopher who believed that all actions should be done according to an underlying principle. The morality of any action should be judged against how closely the action aligns with the underlying principle (Kant & Kroeger, 1882). An example of a Kantian approach to the rights of privacy is found in the famous Supreme Court case *Roe v. Wade* (1973). The Supreme Court held that Texas' anti-abortion law was unconstitutional. Ely (1973) evaluates Justice Blackmun's point that: "The right to privacy, though not explicitly mentioned in the Constitution, is protected by the Due Process Clause of the Fourteenth Amendment. This right is

broad enough to encompass a woman's decision whether or not to terminate her pregnancy." (p. 1)

An opposing view of privacy rights calls upon the fifth century Augustine of Hippo. Augustine sought to justify an all all-powerful and all-loving God existing in and allowing evil in the world. Augustine believed that God remained perfect without being held responsible for evil (Hanson-Smith, 1978). The two were absolutely separate. In Graham Walker's book *Moral Foundations of Constitutional Thought: Current Problems, Augustinian Prospects*, Graham considers that an understanding of the rule of law prevents society from mistaking law for moral truth (Walker, 2014). To people like Walker, the moral approach to a right to privacy is all wrong. Courts should never look to a moral principle in deciding the scope of privacy rights.

Bedi argues against rights to privacy for a completely different reason: he claims those rights are unnecessary. In a recent decision in *Lawrence v. Texas* (2003) the Supreme Court struck down the Texas sodomy law in a 6-3 decision. This Texas law was based solely on morality. Bedi (2005) claims this decision "renders the substantive due process right to privacy obsolete" (p. 39). His reasoning is that a right to privacy "shields behavior while demeaning it" (p. 40). In other words, even though the majority of society may have a moral objection to gay sex, society chooses to tolerate that behavior in the privacy of a bedroom. In his book *Democracy's Discontent: America in Search of a Public Philosophy*, Michael J. Sandel (1996) criticizes the right to privacy as a right because it stigmatizes the act protected by privacy as deviant and abnormal (Fairfield, 1999).

In *Griswold v. Connecticut* (1965) the Supreme Court ruled that a Connecticut law that made it illegal to use a drug for contraception was unconstitutional—that the law violated a right to privacy (Garrow, 2011). Sandel would argue that before the Griswold case nobody questioned

whether a married couple had a right to have sex for the purpose of procreation. After all, that's how babies are made, but the larger point is that the Connecticut law made having sex without the purpose of procreation a morally incorrect act.

Corlett (2002) offered a middle ground to the privacy dilemma by framing a Hybrid Theory of the Moral Right to Privacy. This theory has two principles:

1. Privacy Respecting Principle: where a person is the primary agent of a privacy context, that person's privacy "should be respected to the extent that accessing information about [that person] can in some manner be reasonably expected."
2. Privacy Rejecting Principle: where a person's privacy "may be rejected to the extent that accessing information about [that person] can in no manner be reasonably expected to significantly harm [that person] undeservingly." (p. 340)

These principles are always applied so that priority is given to the respecting of privacy over rejecting privacy. Corlett (2002) believes that applying the principles in this order would prevent the "weighing of harms and benefits" that courts engage in when determining a right to privacy (p. 340). He goes on to write that to cause harm means to have a person's interests set back. If one's privacy is reasonable expected, but not respected so that your concerns have been hampered, then one has been harmed.

## Philosophy of Privacy

In *Privacy and the Right to Privacy*, H.J. McCloskey (1980) writes that the right to privacy while one of the most widely demanded rights today, was overlooked by liberal philosophers:

> John Locke's writings contain no reference to what we now call privacy. Rousseau was evidently insensitive to the claims of privacy. Kant's importance for liberalism lay in his concern for respect for persons; he seems nowhere to have related this to privacy. Wilhelm von Humboldt was preoccupied with securing and defending the individual's liberty, and seemed unaware of privacy as a value (p. 17).

Credit for the relatively new concern for privacy is given to technology-based techniques for systematically and completely gathering private information. The motivation behind liberal thought on privacy was less about creating happiness for the most people, and more about respect that should be shown for the individual. McCloskey claims that Stephen's book Liberty, Equality, Fraternity's brief discussion on privacy (Stephen, 1967) is the only exception to liberal thought about privacy: that privacy relates to the intimate and the delicate and that's why it deserves respect (McCloskey, 1980).

Privacy is often confused with "liberty, autonomy, secrecy, and solitude" (Tivani, 2007, p. 3). Each of these metaphors is a reflection of a particular philosophical thought regarding privacy. They tend to describe privacy or at least what privacy should be. Other philosophical foundations of privacy are rights-based. They describe privacy in terms of a space or zone that can be invaded. Others believe that there is no legal or natural right to privacy. Negley (1966) writes: "What has not been discussed, or at least made clear, is why privacy is commonly considered a right or a value to be protected by the law. There is no historical consensus, in philosophy, politics, or law, that it is such a right." (p. 319)

Not all normative theories on privacy are rights-based. Some like Roger Clarke (1999) believe that it's "often more useful to perceive privacy as the interest that individuals have in sustaining a personal space, free from interference" (p. 60). Personal interests can be intentions or desires in achieving some goal or a desire to enhance one's own well-being. If one views privacy regarding personal information much like a property interest, then it's clear that part or all of that property can be taken away by a breach of trust—bringing the reader back around to social contract theory.

Kasper remarks how in Schoeman's (1992) book *Privacy and Social Freedom*, the author distinguishes between two types of privacy: privacy from, which is intended to restrict access to private information, and privacy for that permits people to "develop themselves and their relationships" (Kasper, 2005, p. 73). Deckle McLean (1995) describes four types of privacy in his book *Privacy and Its Invasion*. Access-control privacy is closely related to secrecy. It's a privacy that entitles one to safe guard any information about the self. Respect privacy can be shared with a group. It's a protection against insults. Room to grow privacy is respect for someone to retreat from the unpleasant or an unkindness. Safety valve privacy is unlike room to grow privacy because it does not require as much solitude. Safety valve privacy is "a response to the discomfort that people must adopt to make their ways in existing society" (p. 65).

Not all scholars see a need for privacy. Critics of privacy sometimes embrace the nothing to hide argument. This argument claims that as long as someone is not doing illegal or immoral acts, then there is nothing to be afraid of, nothing private to defend. Tunick (2013) provides an example of how Internet access to public information can cause unjust punishment: Dateline NBC produced a television show called *To Catch A Predator* where adult decoys posed as young

teens anxious to engage in sexual activity with adult men, arranged through Internet online chatrooms. Typically the show lured adult men to a sting house where cameras would be waiting. Assistant District Attorney Louis Conradt was invited to a sexual rendezvous via an Internet chatroom, but chose not to go to the sting house. Upon seeing NBC cameras and a SWAT team storming his house, "he fatally shot himself, unable to bear the public humiliation" (p. 645).

Skeptics of privacy acknowledge that even if someone does not perform illegal or immoral acts, others can use information about a person in ways that may do harm. For example, the UK Revenue and Customs (HMRC) lost the confidential information of some 25 million people (Crossman, 2008). Solove (2003) makes a point that today, anyone can broadcast another person's "unguarded moments or times of youthful awkwardness to an audience of millions" (p. 2). Companies that archive Internet data can make sure that embarrassing information follows a person for life. Google and other search engines hold private information waiting to be mined.

## How DNSSEC Improves Privacy

DNS is vulnerable to several kinds of attacks capable of interfering with common Internet use. DNSSEC was designed to protect DNS against attacks. This protection is applied through resources records (RRs). A DNS zone can delegate part of its namespace to another zone called a child zone (Pappas, Massey, & Zhang, 2007). For example, uvu.edu can delegate part of its namespace to create tc.uvu.edu. Each zone keeps the RR associated with the names under its stewardship. RRs often contain configuration information for a specific service and are divided by class (C. Liu & Albitz, 2006). Leading up to a discussion of issues with DNSSSEC processes, Wijngaards & Overreinder (2009) discuss several DNSSEC-specific RRs that help

establish a chain-of-trust where each resolver in the DNS hierarchy passes trust to its subordinate using public key infrastructure key-signing techniques. This chain-of-trust works by using secure delegation pointers called Delegation Signers (DSs). The DS record holds a hash of a child's zone public key which is signed by the parent zone's private key. The chain-of-trust always begins with an initial trusted entity known as a trust anchor. There is a security issues involving a flaw in the process of establishing a chain-of-trust: a root public key injection attack on the client side compromises the chain-of-trust. "Any compromise in any of the zones between the root and a particular target name will result in data being marked as bogus, which may cause entire sub-domains to become invisible to verifying clients." (Ariyapperuma & Mitchell, 2007, pp. 6-7) This means that authoritative servers would not be able to directly resolve queries for their domains. Only non-authoritative answers could come from secondary DNS servers. Caching non-authoritative domain servers supply responses to DNS queries are subject to the additional vulnerability of cache poisoning.

Other vulnerabilities arise from the problem of key management. To be secure public-private key combinations have to be updated on a regular basis, known as key rollover. Key pairs can become stale. Guette (2009) writes how key management affects the chain-of-trust:

> Existing key rollover mechanisms only updates keys on the name servers, resolvers that have configured the old keys as trusted are not notified that these keys are being replaced. Consequently, the static key configuration in a resolver raises consistency problems between keys deployed in a zone and trusted keys configured in a resolver. If all keys statically configured in a resolver becomes out

of date, this resolver cannot perform secure name resolution any longer.

(pp. 839-840)

In summarizing the design flaw in DNSSEC Osterweil et al. (2014) write that: "An underlying challenge is that trust in a zone's keys is learned from a DNS hierarchy that was designed to

distribute authority and provide name uniqueness, not provide key verification." (p. 283) In other words, while DNSEC does authentication very well, verifying identity is a completely separate task that DNSSEC was never intended to do.

When describing DNSSEC security states, Wijngaards & Overreinder (2009) identify four possible states of DNSSEC validation. One state, Indeterminate, happens when no trust anchor exists. In this state, a chain-of-trust cannot be built because there is no place to begin. In Bogus, although a trust anchor does exist, responses fail to validate. In this case, trust does not get established. For the Insecure state, there is a trust anchor, but a domain in the chain chose not to extend trust to a subordinate domain. Only in the Secure state is data validated and the DNS resolution considered authenticated.

**Clients Authenticate Signature**

DNSSEC implementation necessitates that domain-name owners provide start-of-authority (SOA) name servers capable of digitally signing data, but in all cases, the onus falls to the client to validate any digitally signed data (Wijngaards & Overeinder, 2009). While Wijngaards & Overeinder contend that client-side validation is the key to preventing Man-in-the-Middle (MitM) attacks, several other authors (Decasper & Plattner, 1998; B. Liu & Lu, 2009; V. Liu, Caelli, Foo, & Russell, 2004) claim that there are still flaws in the digitally signing of data.

**Security Flaws**

Ariyapperuma & Mitchell (2007) write that: "DNSSEC does not guard against poor configuration or bad information in the authoritative name server, and does not protect against buffer overruns or DDoS attacks" (p5). They mention that DNSSEC "suffers from serious security and operational flaws" (p. 1). Additionally, the authors remark that DNSSEC's ability to report errors is minimal, cannot prevent buffer overruns (one of the most common attacks) or DDoS attacks (p. 8). The authors comment that secure delegation of trust is a complex setup. The public/private key combinations used to validate data can be compromised over time. In order to keep public/private key combinations fresh, they should be changed often. Changing keys along the chain-of-trust is easily done except at the root level of the DNS hierarchy. Here, root key rollover is a problem as the root level is often the designated trust anchor in a DNSSSEC chain-of-trust (Friedlander, Mankin, Maughan, & Crocker, 2007).

Key roll-over is only one of several obstacles to security in the DNSSEC authentication process that are significant. One of those significant flaws mentioned by Ariyapperuma & Mitchell (2007) is the lack of a "higher level of time synchronization between the servers" (p. 5).

**Relative Time**

When Mockapetris created the DNS standard (1983b), the time standard established was the number of seconds since the UNIX epoch January 1, 1970. This means that all times in DNS are relative. Ariyapperuma (2007) makes a claim that relative time references are defined in the RFCs for DNS, but there are no time stamp specifications defined in RFC 882 or RFC 883.

DNSSEC creates a need for loose time synchronization because digital signatures or certificates are time stamped. A resolver has to have a similar concept of absolute time in order to determine whether a signature is valid or has expired. If an attacker could change the

recipient's view of the current absolute time, he could trick the resolver into using an expired signature.

The outside possibility that an attacker could trick the client into using an expired signature means that the client could mistakenly accept one DNS answer as valid when it is not, ahead of a legitimate DNS answer to the name query. This technique is a classic MitM attack.

**Man-in-the-Middle**

Man-in-the-Middle (MitM) can be used against any protocol that uses certificates to attempt to secure the communication channel. A popular target of MitM attacks is the Hypertext Transport Protocol (HTTP) combined with Secure Sockets Layer (SSL), or HTTPS. HTTPS uses certificates to attempt to secure the encrypted channel between the web client and the web server. Xia & Brustolini (2005) report that two tools to perform a MitM attack are free available on the Internet: `arpspoof` which will send the client false ARP packets containing the attacker's MAC address mapped to the local router's IP address and `dnsspoof` which sends false packets containing the attacker's IP address associated with a server's domain name. Employing a MitM attack against HTTPS is well documented, as listed by Pansa & Chomsiri (2008):

1. Falsely notifying a gateway-router that the hacker machine is a victim
2. Notifying the target machine that the hacker machine is a gateway-router
3. Enable a packet routing feature on the hacker machine
4. Running a DNS spoof to force the victim to connect to a HTTP or HTTPS port on the hacker machine
5. Distributing a false certificate to the victim machine
6. Communicating with the victim machine using a false certificate

7. Now communicating with the HTTPS web server using a genuine certificate obtained from the HTTPS web site
8. Transmitting the parameters and data between the victim and the HTTPS server
9. The hacker records the data transferred between the victim machine and the HTTPS server
10. The hacker now has the data (p. 22)

DNSSEC is also a protocol that attempts to secure the communication channel through the use of certificates. Ariyapperuma & Mitchell (2007) remark that DNSSEC has the ability to detect MitM attacks through data original authentication or transaction and request authentications. While the authors are technically correct about being able to detect alterations in the receiving certificate, there are so many certificates to verify, that a hacker doesn't have to be able to fool a client every time. Through many repeated attacks on a client, a hacker can redirect a client to a bogus replicated site. Having led the victim to a bogus site with a seemingly valid certificate, the hacker provides an interactive site to pry security credentials from the victim (Amir Herzberg & Jbara, 2008; Qi, Tang, & Wang, 2008). Additionally, Herzberg & Jbara (2008) cite a study [Gabrilovich and Gontmakher 2002] showing that hacker success rates are 50% for picture-in-picture fake web sites and 37% for the homographic fake web site (p. 16:5).

In a paper titled *Security Analysis on Mutual Authentication Against Man-in-the-Middle Attack*, Chen, Guo, Duan & Wang (2009) write that: "Unilateral authentication is vulnerable to the Man-in-the-Middle (MitM) attack. The security of mutual authentication against MitM attack is also weak" (p. 1855). Oppliger, Rytz, & Holderegger (2009) remark that: "In spite of their practical significance, only a few technologies and mechanisms effectively protect against MitM attacks." (p. 28) HTTPS and DNSSEC are two protocols used to demonstrate the vulnerability

from MiTM, but even encrypted channels are subject to MitM attacks. Ahmad (2008) cites examples where MitM is possible against users connecting to secure shell (SSH) servers that use vulnerable versions of Open SSL (p. 72).

### Address Resolution Protocol Poisoning

Trying a MitM attack against HTTPS is so common that there is a specific tool: `WebMitM` used to simplify the attempt. Using `WebMitM` the attacker generates a new certificate that will be accepted by the web client as valid as if it were generated by the appropriate web server. If the client accepts the certificate, the attacker will be able to intercept and decrypt all traffic sent by the client. It doesn't even matter if the client is on a switched local area network (LAN). By maliciously modifying the Address Resolution Protocol (ARP) table, the client always thinks it is communicating with the correct Internet Protocol (IP) address. This is called ARP poisoning or ARP spoofing. Once ARP spoofing is accomplished, the attacker can intercept any DNS requests from web clients for manipulation. Coupled with a DNS spoof, the attacker's goal is to have all traffic between the web client and server pass through the attacker's machine (Ford, 2009, p. 79).

### Spoofing and Redirection

ARP spoofing is only the beginning for an attacker. Other elements of the communication channel can be used for a type of identity theft. "As for identity spoofing, the attacker can play the roles of both client and server at the same time, eavesdrop, modify, delete, redirect, replay and forge the 'real'communication messages between client and server" (Chen et al., 2009, p. 1856). It's common for users to not notice a wrong Uniform Resource Locator (URL). Herzberg (2008) claims the primary reason is two-fold: naïve users are not aware of the

structure of a URL and its relationship to domain ownership; the other is that most users do not manually type in URLs, they follow links from one URL to another.

**Making the Channel Insecure**

Once a MitM attack has been successful, the communication channel is insecure. To hide this fact, the MitM attacker may re-establish new, secure communication channels: one between the attacker and the client and another between the attacker and the server. This is referred to as the Dolev-Yao threats model (Oppliger et al., 2009). Oppliger & Holderegger go on to make the point that many people believe that although an attacker can passively or actively attack the message going back and forth between the client and server, the attacker cannot attack the end points of the channel. The authors say that this is not the case, that the attacker has many ways to directly attack the client. Uusitalo (2009) claims that user experience as a type of cost is one reason for the prevalence of the MitM attack: more secure methods of establishing a communication channel are more complex for the average user.

**Certificates**

Oppliger & Holderegger (2009) claim that effective protection against online channel-breaking attacks like MitM, require transaction-authentication technologies like the use of certificates. However, Herzberg (2008) remarks that all an attacker has to do to bypass the certificate as an authentication technique, is to get the client to accepted a certificate issued by a Certificate Authority (CA) trusted by the client, but issued by the attacker. This illustrates a common problem: most users do not read issued certificates closely. Ford (2009) reminds us that if a certificate isn't trustworthy, the entire communication path is vulnerable" (p. 78). Oppliger & Holderegger (2009) levy some of the blame on the complexity of modern browser

interfaces. They suggest simplifying certificate validation processes in browsers would reduce the vulnerability from MitM attacks.

Another problem with certificates as an authentication technique, as pointed out by Ahmad (2008) is that certificates with "weak keys issued by trusted CAs are valid until they expire, even if they're revoked" (p. 71). Kaminsky (2008) showed how DNS redirection techniques are easily accomplished, especially if the server has a weak certificate.

Just checking that the lock icon exists at the bottom left of the browser is not enough to verify a proper certificate. Tan (2007) tells how a scam targeting Earthlink users involved attackers taking the effort to register a real certificate for the phishing website. This extra step caused a bona fide lock icon to appear in the victim's browser. The bona fide certificate authenticated that indeed, the victim was at a web site replicating the Earthlink web site. Only a careful check of the URL would have revealed the scam. An issued certificate does not mean that the victim is at the intended URL (Qi et al., 2008). Pansa (2008) illustrates that it is easy to issue fake certificates to deceive victims into revealing private information sent over HTTPS.

**Digital Certificates: Problems With Trusts and Anchors**

Certificate vulnerability at both ends of the communication channel is not the only challenge facing certificates used for authentication. One challenge pointed out by Sweden (2008) is that there is not a good way to distribute the public keys of signed DNS zones to their unsigned parents, establishing a chain-of-trust. Additionally, push back is being experienced from DNSSEC implementation because the chain-of-trust is an added structure to the DNS framework, it's more work and the process is not standardized. Once having established the trust, the trust might last too long – this is particularly true of the root domain as a trust anchor.

Wouter (2008) adds that it's "impossible to distribute all the zone owner's public keys to all DNS validators a priori" (p. 37).

There have been several proposals offered in the literature that modify the distributed trust model to overcome this key distribution problem inherent in asymmetric cryptography. HerzberG (2008) suggests deploying the PGP Web-of-trust model proposed by Zimmerman (1995). The PGP Web-of-trust model makes peers responsible for validating certificates, somewhat by-passing the commonly used chain-of-trust.

**Certificates Not Authenticated**

Another certificate vulnerability discussed in the literature is that certificates can be issued to hackers. Both SSL and TLS rely on the Public Key Infrastructure (PKI) that includes CAs needed to issue certificates. The public key of a web site is authentic if its certificate's digital signature is validated against the public key of the CA (Tan, 2007, Wouter, 2009).

If a MitM attacker cannot get the private key of a server, the attacker creates a new certificate containing his own public key and sends it to a potential victim. The victim will generate a secure session key and encrypt it using the MitM attacker's certified public key (Chen et al., 2009). The attacker's public key was certified by the attacker's own CA. Ford (2009) claims that it is so common for entities to sign their own certificates with their own CA, that users have become accustomed to ignoring the certificate warning messages.

Additionally, Ahmad (2008) points out that the web security system relies on responses from web administrators when certificate authorities offer replacements for weak certificates. Responses have traditionally been very slow. This is troubling when current browsers have no way to check to see if certificates have been replaced or revoked. An attacker doesn't necessarily have to create their own certificate, just use a revoked certificate that has not yet expired.

But not all of the responsibility falls on web administrators not replacing revoked certificates. Osterweil, Pappas, Massey, & Zhang (2007) point out that DNSSEC has no built-in procedure to handle a situation where a zone's private key has been lost or compromised. While an administrator could remove the availability of the public key in the key pair, it does not remove the compromised key from the DNSSEC system.

Ahmad (2008) claims that this situation "is a dress rehearsal for a large-scale compromise within the global PKI that could occur in the near future" (p. 73).

### Device-specific Certificates

The inability of the enduser to check on certificates themselves is a problem addressed in the literature. Forzberg (2007) suggests a CA and naming infrastructure based on device-specific certficates. However, he recommended retaining the current DNSSEC infrastructure that utilizes domain-specific certficates so that a Start of Authority (SOA) can authenticate itself as the authority for a particular domain. Pansa (2008) also agrees with the idea of device-specific certificates, adding that the device should be the network card with both the private and public keys be created during the production process at the factory.

## Authentication

### Client-side Verification Required

The reason so much attention is being paid to certificates, is because certificates are the way DNSSEC authenticates. Kim, et al. (2008) concisely sum up the role of authentication when they wrote: "Particularly, [the] authentication process is an essential requirement for [the] client to receive services provided by [the] server" (p. 18).

Chen (2009) remarks that authentication that is one-sided is vulnerable to the MitM attack. Even mutual (client and server) authentication is weak against the MitM attack. Mutual

authentication plays such a crucial role in establishing a secure communication channel, that considerable effort is being put into developing secure protocols. With both the client and the server establishing a communication channel, both entities need to verify the identity of the other (Forzberg, 2008). However, even secure protocols developed to standard documents often contain security flaws such as MitM, replay attacks, parallel session attacks, and reflection.

**Time-based Authentication is Vulnerable to MitM**

Authentication mechanisms that use time stamps attempt to use synchronized time between server and client. This synchronization experiences problems of time deviation due to latency (Kim et al., 2008). The time synchronization problem is further frustrated by DNSSEC because DNSSEC uses time stamps for certificates based on a relative time mechanism held over from the original DNS specifications in RFC 883. The relative time is always measured in seconds from the UNIX Epoch January 1, 1970 (P. Mockapetris, 1983a, 1983b).

The time deviation problem exposes authentication mechanisms like DNSSEC to various attack methods like spoofing attacks, and variations on the replay attack such as the MitM. The problem is that these mechanisms "cannot provide confidentiality and non-repudiation." (Kim et al., 2008, p. 19)

Challenges to authentication mechanisms can be especially difficult to detect because they are capable of being just good enough for a long time and nobody notices. Ahmad (2008) points out that a patch for Open SSL key generation containing a vulnerability went unnoticed for two years before it was caught by Argentinian researcher Luciano Bello. Although keys appeared random, there wasn't enough randomness in the keys produced. This meant that a hacker could generate all of the key pairs possible used by that version of Open SSL.

## Vulnerability Costs

### Security Vulnerabilities Affect Everyone

Ahmad (2008) goes on to explain the costs of this OpenSSL vulnerability that went unnoticed for two years:

> The consequences of this vulnerability were, and still are, wide ranging, from affecting users who browse the Internet and shop or bank online to system administrators who are responsible for ensuring secure communications and the integrity of their systems and data (p. 71).

Endusers are responsible for the part of the costs of security vulnerabilities too. After a Spanish bank was the victim of a picture-in-picture spoofing attack, eighty percent of Spanish Internet users did not change their online banking habits and 73.1% continued to make online purchases (Uusitalo et al., 2009). However, despite a seemingly apathetic approach to online security by endusers, there is a growing perception that the Internet is an unsecure place to do business (Parameswaran, 2007).

Herzberg (2008) cites studies by Dhamija et al. 2006 and Wu, et al. 2006 that show most users are not able to recognize even the most basic signs of a breach in the security of their Internet interaction. Parameswaran (2007) adds that the growing availability of inexpensive Internet devices and broadband connectivity has made large scale attacks possible including the remote hijacking of computing systems.

### Dollar Figures, Loss of Goodwill

Although costs in dollar amounts are high, Uusitalo, et al. (2009) estimates that the overall loss of reputation to a targeted financial organization exceeds any real costs. Amir, Herzberg & Jbara (2008) cite a study by Gartner Research [Litan, 2004] that spoofing attacks

caused two million users to provide authentication information to hackers. The resulting authentication breech resulted in a $1.2 Billion in direct losses to U.S. banks and credit card companies just in 2003.

**MitM Attacks Will Continue**

The possibility for MitM attacks will continue as long as there are vulnerabilities in using certificates as part of an authentication system like DNSSEC (Ahmad, 2008). Weak certificates, channel breaking attacks, and time synchronization problems are all vulnerabilities that are yet to be addressed. Empirical research is needed to investigate whether adding an absolute time reference to the DNSSEC authentication mechanisms can diminish or eliminate the MitM threat.

# CHAPTER 3

## METHODOLOGY

This chapter offers the research methodology of the technical experiment and presents (a) the experimental design of the study, (b) the participants of the study, (c) settings and apparatus, and (d) the data collection and data analysis.

### Experimental Design of the Study

If all DNSSEC can do is validate responses between servers, then DNSSEC may not provide secure name resolution the way that the designers intended. The DNSSEC client should not attempt to navigate to URLs where the DNSSEC response is not validated (Arends, 2005, Sec. 5.5).

This study utilized a simple quantitative experimental design. Evaluating the performance of DNSSEC client validation, this study investigated the way DNSSEC clients responded to DNSSEC PKI packets that had been altered. The intention of the study was to answer research questions concerning whether a DNSSEC client would first, acknowledge a non-valid name resolution response and second, correctly fail to load a HTML page from a non-validated URL where the DNSSEC server's Zone Signing Key (ZSK) (public key of the Public Key Infrastructure pair) had been compromised. The study also observed the influence the Network Time Protocol (NTP) had on the DNSSEC Resource Record's (RR) time stamp used in

the server's ZSK and whether that influenced the DNSSEC client in not loading a non-validated URL.

## Participants of the Study

The population in this study is very large. The population is every name resolution response to a query made from a DNSSEC server or DNSSEC stub resolver with or without the benefit of NTP time stamps. The participants of the study were a sampling of the population. The sample chosen was sequential and non-random with and without NTP installed and configured. Cochran (1963) provides a formula for determining the sample size for large populations:

*Equation 1*. Sample size formula for large populations.

$$n_0 = \frac{Z^2 pq}{e^2}$$

Israel (2009) suggests an application of the formula where $n_0$ is the sample size, $Z^2$ is 95% of the sample means within two standardized deviations, e is the level of precision wanted, "p is the estimated proportion of an attribute that is present in the population, and q is 1-p." (p. 3) P=0.5 will be used for maximum variability since the variability in the sample means is unknown. A 95% confidence level is wanted as well as a $\pm$5% precision. The equation now yields a sample size of:

*Equation 2*. Sample size formula for large populations with values.

$$385\ samples = \frac{(1.96)^2(0.5)(0.5)}{(.05)^2}$$

The substantive research question that emerged that this study sought to answer with a sampling size of 385 iterations in two settings was: Does using an absolute time stamp in the

signature and inception fields of the Resource Record Signature (RRSIG) of a DNSSEC certificate (public key) provide any real benefits to securing DNSSEC in the creation of PKI certificates between DNSSEC clients and servers?

The research hypothesis was that using an absolute time stamp from a NTP daemon referencing an atomic clock would make a difference in the DNSSEC client's behavior when presented with an invalid name resolution response.

$H_0$: There is no difference in the behavior of a DNSSEC client when using a relative timestamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

$H_a$: There is a difference in the behavior of a DNSSEC client when using a relative time stamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

## Instrumentation and Measures

The research consisted of six steps as follows: (a) a session was established between the DNSSEC client and DNSSEC server by typing in the address of a dedicated URL, jeffdiss.org, (b) the response was validated by the display of a green key in the address bar, (c) the DNSSEC client's cache was cleared, (d) the Kjeffdiss.org.+005+50340.key file was modified by changing at least one character in the RRSIG entry for the public key on the DNSSEC server, (e) the named daemon on the DNSSEC server was restarted so the new file would be read, and (f) a new browser session was established with the same URL (jeffdiss.org) and the validation key and web page were observed.

### Background

Early attempts were made at testing the vulnerability of an actual Man-in-the-Middle (MiTM) attack that would intercept session traffic between the stub resolver (SR) and the

DNSSEC server. Originally this was to happen within a virtual network setup within the University of Utah's Emulab. The authoritative response headed for the DNSSEC client would be redirected and altered en-route. To accomplish this required a modification of the source code of `Net::DNS::DNSSEC`, free-and-open source software. The modified software would be the basis for a Replay Attack Server. A simplified drawing of early attempts is illustrated in Figure 2.

.

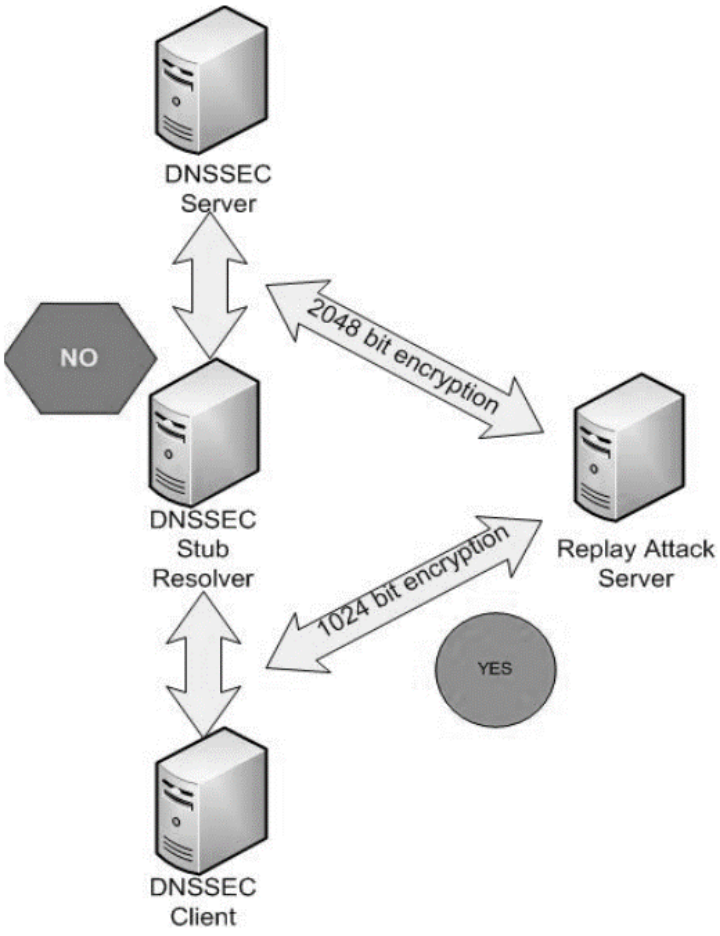


*Figure 2*. Simplified Drawing of Early Attempts. A successful attack will display a green YES on the client's Web browser. A failed attack will display a red NO on the client's Web browser.

Over a period of several years, the research team on this project discovered that the experiment is not whether the hash can be changed; it can and should be expected to be changed if the MiTM is successful, but rather how the client responds to that change. A personal entry in the research notes by Shawn Anderson, Research Assistant reveals that:

> With DNSSEC seeming to work well, the next step was to try and figure out if the client would reject a DNS response that was not signed. This has turned out to be one of the cruxes of this research. Because DNSSEC is not widely used and the root servers are not signed, neither current browsers nor current operating systems have been designed to reject unsigned DNS responses. The Firefox plug-in only allows a user to see if the response is signed, but does nothing to prevent spoofed DNS responses (Anderson, 2012, para. 7).

In an email correspondence between Kyle Law, Research Assistant and the DNSSEC mailing list, a response from Jim Reid (2012) explains:

> The DNSSEC protocol is very clear how validation failures are handled: **return SERVFAIL**. Whether some client or application gives up at that point or does something else is for that application to decide. This may or may not be influenced by the prevailing local validation policy, if there is such a thing.

The original research plan was to modify the Transition Signature (TSIG) of the DNSSEC response to the client, causing a valid MiTM. Further investigation revealed that the TSIG only protects server-to-server communication, not server-to-client communication (Nixcraft, 2009). Attempts to modify the code in the `Net::DNS::DNSSEC` application, and another tool Ettercap with DNSSEC modules did not result in a tool that could intercept session

packets. Rather than trying to create a real MiTM attack through packet interception, we realized that if the MiTM attack were assumed and the public key directly modified, then we could focus on the DNSSEC client's response to the attack.

Working with the University of Utah's Emulab presented an operational challenge. It took about 30 minutes for the virtual network (VLAN) creation script to load to establish the hosts and virtual network links between them. Inactivity of more than 10 minutes saw a re-allocation of server resources to other projects. What became apparent was a need for a dedicated research asset, so plans were made to change the research equipment.

**Apparatus**

To meet the test objective of testing DNSSEC sessions, a DNSSEC VPS was set-up using the GoDaddy! hosting service. The server not only provided DNSSEC name resolution via the Berkely Internet Naming Daemon (BIND) 9.8.2, but also hosts a single, simple web page using Apache 2.2.15. The server's operating system was CentOS Linux 6.4 final.

The DNSSEC server used a dedicated registered domain: **jeffdiss.org**. This domain was established within the DNSSEC chain-of-trust for the **.org** TLD. Each time the browser cache was cleared and directed to jeffdiss.org, a DNS stub resolver (SR) passed the name resolution request on to one of 13 world-wide root servers that then passed the request down the DNS hierarchy to a TLD server and then on to the master DNS server providing an authoritative response for jeffdiss.org. Per RFC 2065, communication sessions between DNSSEC servers used a 2048 Rivest, Shamir and Adleman (RSA) Zone Signing Key (ZSK) and communication sessions between the SR and the browser used a 1024 bit RSA Key Signing Key (KSK).

The DNSSEC client was a personal computer (PC) laptop, Hewlitt-Packard (HP) dv6-6153cl running Windows 7 Pro and the Firefox browser version 31.0b1. The authoritative DNS

response from the web server jeffdiss.org was validated with a plug-in called DNSSEC/TLSA Validator version 2.2.0.1 by CZ.NIC Labs. The validator plug-in presents a green key in the browser's address bar when the DNSSEC signed records are validated up through the DNSSEC hierarchy.

> DNSSEC/TLSA Validator allows you to check the existence and validity of DNS Security Extensions (DNSSEC) signed records. If a valid DNSSEC chain related to the domain is found the plug-in will also check for the existence of Transport Layer Security Association (TLSA) records. TLSA records store hashes of remote server TLS/SSL certificates. The authenticity of a TLS/SSL certificate for a domain name is verified by the DANE protocol (RFC 6698). DNSSEC and TLSA validation results are displayed by using several icons as shown in Figure 3. Clicking on a given icon symbol reveals more detailed information ("DNSSEC/TLSA Validator", 2011, p. 1).

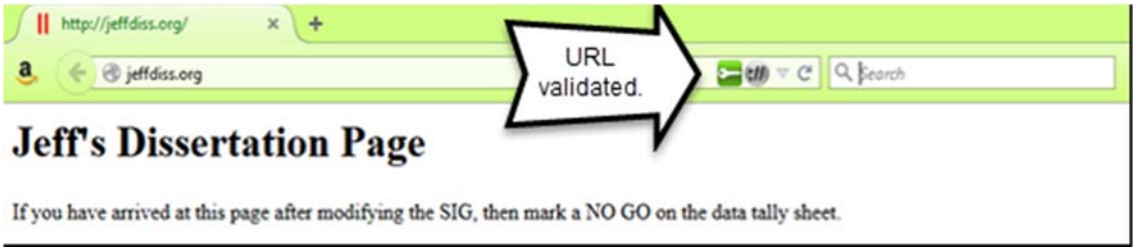


*Figure 3*. The DNSSEC/TLSA Validator. The DNSSEC/TLSA Validator shows a green key in the address bar of the browser when the URL is validated.

The selection of the communication sessions between the DNSSEC client and server was sequential and nonrandom. The test scenario assumed that a hacker had unfettered access to modify the RRSet to change the public key validating the DNSSEC server response. For each session, the DNSSEC server was validated first by the DNSSEC/TLSA Validator and the

DNSSEC client cache was emptied. Next, the public key on the DNSSEC server was modified by at least one character and validation was attempted again on the DNSSEC client using the DNSSEC/TLSA Validator. The session testing ran for 385 iterations first without the Network Time Protocol (NTP) implemented on the DNSSEC server and then for 385 iterations with NTP providing an absolute time stamp. Figure 4 shows a graphical representation of the experiment.

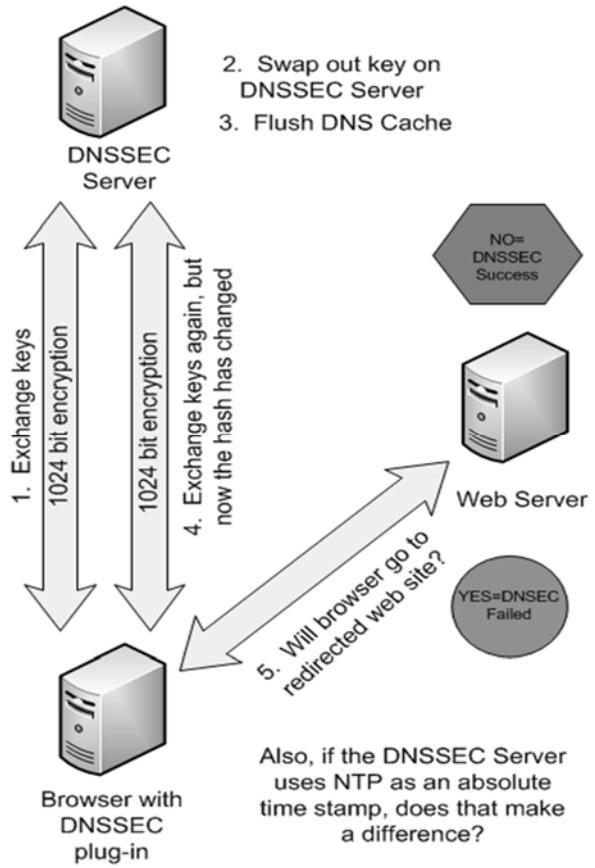


*Figure 4*. Drawing of the Experiment Design. The experiment begins with a successful MiTM attack. A DNSSEC-enabled browser attempts to go to a redirected web site. This is done with and without NTP influencing the TSIG field of the DNSSEC Server.

**Independent Variable**

The independent variable in this study was the time stamp used in the name resolution response certificate, using either an NTP absolute time or the relative Unix epoch time.

The two configuration test scenarios A and B in Table 1 represented the setup planned for the experiment. Sessions lasting only seconds were briefly established between each participant in the DNSSEC communication chain. During the session, signed certificates were exchanged and name resolution information was passed. However, the experiment began with an altered hash in the TSIG field of the DNSSEC server's zone file to simulate that a successful MiTM attack had occurred. It was important to test the efficacy of the DNSSEC client with and without a time stamp from NTP. Some of the literature has suggested that an absolute time stamp could cause DNSSEC to more readily recognize that a MiTM attack had occurred. In Table 1 the first row shows the 1024 bit encryption of the KSK for the communication-to-server communication. The encryption is a higher 2048 bit for DNSSEC server-to-server communication in the ZSK. The first column shows the two different time stamp references used.

Table 1. Independent and Dependent Variables

| | Configuration | |
|---|---|---|
| | A | B |
| Time Stamp Method | 1024 bit | 1024 bit |
| NTP | Yes | No |
| Unix | Yes | No |
| | Success, Target URL Blocked | |

**Dependent Variables (Measures)**

The dependent variable measured was the success or failure of the DNSSEC client loading a web page at a targeted URL after receiving a name resolution via DNSSEC with an altered KSK in the zone file. Each test iteration was conducted from a DNSSEC client using a DNSSEC/TLSA validator plug-in. The plug-in validated that DNSSEC was protecting the name resolution. If the hash was altered, then the DNSSEC/TLSA validator plug-in should have indicated that fact and the client should not have loaded the redirected web site. We began each test iteration with a simulated successful MiTM attack. When the client displayed the redirected web site, then DSNSSEC did not prevent what it was designed to prevent: a highjacking of web client traffic to alternate web sites.

## Data Collection and Analysis

Without the NTP daemon configured and pulling a time synchronization from the U.S. Naval Observatory, the master server used the default UNIX Epoch as its time reference, the number of seconds since January 1, 1970. With the default UNIX Epoch time method, a simple tally sheet was kept for 385 test run iterations. If the DNSSEC client displayed the target URL

even when the name resolution is non-validated, then a check mark was placed in the Configuration A column. If the DNSSEC client did not display the target URL because the name resolution response was not validated, then a check mark was placed in the Configuration B column. This same technique was repeated again with the NTP daemon loaded and configured, which provided an absolute time stamp. Table 2 is an example of collated sample data.

Table 2. Example of Collated Data

| Method | DNSSEC using UNIX epoch time | DNSSEC using NTP time |
|---|---|---|
| Client certificate | 1024 bit RSA ZSK | 1024 bit RSA ZSK |
| Successful | 711 | 654 |
| Unsuccessful | 89 | 146 |

Table 2 shows the numerical values from experiments using Configuration A and B displayed in Table 1. Each Successful count in Table 2 represents the DNSSEC client accessing the target URL even though the KSK was altered. Each Unsuccessful count in Table 2 represents an instance where the DNSSEC client rejected the DNSSEC response and did not try to access the target URL. To test the null hypotheses, the statistical technique that was used was proportion analysis and Fisher's exact test (Fisher, 1922). Here, the independent (predictor) variables are categorical.

The purpose of this proposed research was to determine the performance of DNSSEC name resolution validation and the influence of using NTP on that performance. This study provided statistical analysis on whether an intentionally corrupted session certificate changed the

behavior of a DNSSEC client and whether the use of an absolute time stamp influenced that behavior.

# CHAPTER 4

# RESULTS

Shue & Kalafut (2013) recently remarked: "While prior work has examined the DNS from many angles, the resolver component has received little scrutiny" (p. 1). For this research, an experiment was created to determine what influence NTP has on a DNSSEC client's ability to securely resolve a hostname. This study provided statistical analysis on whether an intentionally corrupted session certificate will change the behavior of a DNSSEC client and whether the use of an absolute time stamp would influence that behavior. This was done using two different time stamp techniques: a relative Unix epoch time stamp and a NTP absolute time stamp in the session certificate.

## Population of Study

The research question investigated in this study asks what influence if any, the NTP has on DNSSEC client behavior. The population of interest consists of every name resolution response to a query made from a DNSSEC server or DNSSEC stub resolver on behalf of the DNSSEC client. Even though following Cochran's (1963) suggestion would have calculated a minimum sample size of 385 iterations for a large population, in this study 800 iterations were collected in a 48 hour time period for each setting. The parent population is all DNSSEC client name resolution queries and responses received in 48 hours. The parent population is large and the exact number is unknown. Just the Google public DNS server gets 140 billion query requests

in 48 hours (J. K. Chen, 2012). Eight hundred iterations were chosen to ensure an accurate representation of the parent population, as well as meaningful generalization of the sample results over the entire population.

Therefore, the problem this research investigated was whether using NTP affects DNSSEC client security performance.

## Null and Alternative Hypotheses

The alternative hypothesis (research hypothesis) presented was that using an absolute time stamp from a NTP daemon referencing an atomic clock would make a difference in the DNSSEC client's behavior when given a corrupted session certificate in the DNSSEC resolution response. Therefore, the null and alternative hypotheses are respectively:

$H_0$: There is no difference in the behavior of a DNSSEC client when using a relative timestamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

$H_a$: There is a difference in the behavior of a DNSSEC client when using a relative time stamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

To analyze the data, the first statistical technique used was the z-test of the difference between the two population proportions. This test is appropriate for this experiment because the data are nominal. Therefore, the only meaningful computation is to count the number of occurrences of each type of outcome and calculate proportions. Consequently, the parameter to be tested and estimated is the difference between the population proportions $P_1 - P_2$. The sample proportions $\hat{P}_1$ and $\hat{P}_2$ are calculated from sample data. The null and alternative hypotheses above can be specifically restated in terms of $P_{Unix}$ and $P_{NTP}$ as follows:

$H_0$: $P_{Unix} = P_{NTP}$ or equivalently $H_0$: $P_{Unix} - P_{NTP} = 0$

The alternative hypothesis is that Unix and NTP have different proportions of successfully rejecting the target URL:

$H_1$: $P_{Unix} \neq P_{NTP}$ or equivalently $H_1$: $P_{Unix} - P_{NTP} \neq 0$

**Hypothesis Testing and Confidence Interval**

The alpha will be set at $\alpha = 0.05$. This is a somewhat high alpha, which makes for a higher probability of a Type I error (rejecting $H_0$ when true) and a lower probability of a Type II error (failing to reject a false $H_0$) than using an alpha of 0.01. This alpha was selected because the costs associated with a Type II error are relatively high for original research. It is more important to avoid a Type II error than a Type I error. The large sample size will reduce the chance of a Type II error and increase the Power of the statistical analysis.

The statistic $\hat{P}_1 - \hat{P}_2$ is an unbiased consistent estimator of the parameter $P_1 - P_2$. Since the sample sizes are large enough so that the sample requirements $n_1\hat{P}_1$, $n_1(1-\hat{P}_1)$, $n_2\hat{P}_2$, and $n_2(1-\hat{P}_2)$ are all greater than or equal to five, the statistic $\hat{P}_1 - \hat{P}_2$ is approximately normal. Consequently, the test statistic is:

*Equation 3.* Z-test statistic.

$$Z = \frac{(\hat{p}_1 - \hat{p}_2) - (P_1 - P_2)}{\sigma_{\bar{p}1-\bar{p}2}}$$

where $\sigma_{\hat{P}_1-\hat{P}_2} = \sqrt{\frac{P_1(1-P_1)}{n_1} + \frac{P_2(1-P_2)}{n_2}}$ is the standard error of $\hat{P}_1 - \hat{P}_2$ .

But since $P_1$ and $P_2$ are unknown population parameters, the standard error of $\hat{P}_1 - \hat{P}_2$ is estimated from the sample data. The null hypothesis states that $P_1 - P_2 = 0$; this allows us to pool the data from the two samples to produce an estimate of the common value of the two

proportions $P_1$ and $P_2$. The pooled proportion estimate is $\hat{P} = (x_1 + x_2)/(n_1 + n_2)$. Thus the estimated standard error of $\hat{P}_1 - \hat{P}_2$ is:

*Equation 4*. Estimate of the standard error.

$$\hat{\sigma}_{\hat{P}_1 - \hat{P}_2} = \sqrt{\frac{\hat{P}(1-\hat{P})}{n_1} + \frac{\hat{P}(1-\hat{P})}{n_2}} = \sqrt{\hat{P}(1-\hat{P})(\frac{1}{n_1} + \frac{1}{n_2})}$$

Therefore the test statistic is:

*Equation 5*. Z-test statistic with estimate of the standard error.

$$Z = \frac{\hat{P}_1 - \hat{P}_2}{\sqrt{\hat{P}(1-\hat{p})(\frac{1}{n_1} + \frac{1}{n_2})}}$$

In the study, $x_1 = 711$, $x_2 = 654$, $n_1 = 800$, and $n_2 = 800$, and so $\hat{P} = (711 + 654)/(800 + 800) = 1365/1600 = 0.85313$, while $\hat{P}_1 = (711/800) = 0.888875$ and $\hat{P}_2 = 654/800 = 0.8175$. The value of the test statistic is then:

*Equation 6.* Z-test statistic with estimate of standard error using values.

$$Z = \frac{0.88875 - 0.8175}{\sqrt{(0.85313)(0.14687)(\frac{1}{800} + \frac{1}{800})}} = 4.03$$

At the 5% level of significance, the two-sided critical values are ± 1.96. Since the value of the test statistic **4.03 > 1.96**, we reject the null hypothesis. There is sufficient evidence to support the alternative hypothesis and infer that the two proportions of successfully rejecting the target URL for the Unix and NTP time stamps are different.

In addition, for a two-sided test:

*Equation 7*. Calculating p-value for a two-sided test.

p-value = $2p(z > |4.03|) = 2(0.5 - 0.5) = 0$.

Once again p-value = 0, α = 0.05, so we have overwhelming evidence that the null hypothesis should be rejected. Moreover, the 95% confidence interval for $P_1 - P_2$ (the difference between the two population proportions) is:

*Equation 8.* Two population proportions statistic.

$$(\hat{P}_1 - \hat{P}_{2)} \pm Z_{0.975}\sqrt{\frac{\hat{P}_1(1-\hat{p}_1)}{n_1} + \frac{\hat{P}_2(1-\hat{p}_2)}{n_2}}$$

where $\hat{P}_1 = 0.88875$, $\hat{P}_2 = 0.8175$, and $Z_{0.975} = 1.96$ therefore:

*Equation 9*. Two population proportions static with values.

$$(0.88875 - 0.8175) \pm 1.96\sqrt{\frac{(0.88875)(0.11125)}{800} + \frac{(0.8175)(0.1825)}{800}}$$

= 0.07125 ± 0.03451 and so the lower confidence limit (LCL) and the upper confidence limit (UCL) are respectively LCL = 0.03674 and UCL = 0.10576.

**The Confidence Interval**

We are 95% confident that the interval 0.03674 to 0.10576 covers the true difference in the population proportion of successfully rejecting the target URL from a Unix epoch relative time stamp versus a NTP absolute time stamp in the session certificate. Since zero is not included in this confidence interval, we reject $H_0$ and reach the same conclusion stated above.

**Fisher's Exact Test**

As an alternative statistical technique, let us apply Fisher's exact test. "Fisher's exact test is a statistical test used to determine if there are nonrandom associations between two categorical variables." (Weisstein, 2015, para. 1) This test is useful as a two-proportion test because it is accurate for all sample sizes, whereas the z-test for two proportions is based on normal approximation to the binomial may be inaccurate when the number of successes are smaller than

five and when the number of trials minus the number of successes is less than five. One should note that Fisher's exact test is based on the hypergeometric distribution. Therefore, its p-value is conditional on the marginal totals of the two-way classification table.

Fisher's test statistics is given by:

*Equation 10*. Fisher's Exact Test.

$$X^2 = \frac{n(ad - bc)^2}{(a + c)(b + d)(a + b)(c + d)}$$

for the two-way classification as shown in Table 3:

Table 3. Model of Two-way Classification

| | | | Row Total |
|---|---|---|---|
| | a | b | a+b |
| | c | d | c+d |
| Column Total | a+c | b+d | n |

In this study, the two-way classification is shown in Table 4.

Table 4. Two-way Classification

| | Unix relative time | NTP absolute time | Row Total |
|---|---|---|---|
| Successfully opened target URL | 711 | 654 | 1365 |
| Unsuccessful, rejected target URL | 89 | 146 | 235 |
| Column Total | 800 | 800 | 1600 |

Therefore, the test statistic is:

*Equation 11*. Fisher's Exact test with values.

$$X^2 = \frac{1600[(711)(146) - (654)(89)]^2}{(711 + 89)(654 + 146)(711 + 654)(89 + 146)} = 16.2058$$

The sampling distribution of the test statistics is approximately equal to the theoretical chi-squared distribution. This approximation is appropriate since our sample sizes are large. The chi-square critical value with one degree of freedom at the 5% level of significance is 3.84. Since the value of the test statistic is 16.2058 which is larger than 3.84, we reject the null hypothesis. There is sufficient evidence to support the alternative hypothesis and infer that the two proportions of unsuccessful for the Unix and NTP time stamps are different. The relationship between the z-test statistic for the difference between two proportions and Fisher's exact test is quite interesting. Notice that $\sqrt{16.2058}$ = 4.026 which is the Z-test statistic.

# CHAPTER 5

# CONCLUSIONS AND RECOMMENDATIONS

## Restatement of the Problem

Even before the 2009 Black Hat Conference when Dan Kaminsky famously divulged how a flaw in the foundation of the DNS protocol made nearly all DNS servers susceptible to DNS cache poisoning as documented in Vulnerability Note VU#800113 (DNS vulnerable to cache poisoning, 2008). DNS security had become an interest in technology circles. By the latter part of 2006 NIST had mandated the implementation of DNSSEC in all moderate and high impact federal government IT systems (NIST, 2009a). However promising DNSSEC may be to securing name resolution services on the Internet, DNSSEC certificates that provide authenticity and integrity can be forged (Basu & Muylle, 2003; Dijk et al., 2007; Wu & Zhou, 2011).

When intercepting name resolution traffic, a hacker can successfully issue a MiTM attack because of DNSSEC's default relative time. By using an absolute time stamp DNSSEC will be more secure by making it harder to create a MiTM attack. DNSSEC clients should be able to validate that name resolution responses are bona fide. Therefore, the problem this research investigated was whether using NTP affects DNSSEC client security performance. The hypotheses under investigation were:

$H_0$: There is no difference between using a relative time stamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

By sampling more than twice the minimum samples needed to represent a very large population of signed-domain Internet use, two statistical techniques were used to show that the null hypothesis can be rejected.

$H_a$: There is a difference between using a relative time stamp or an absolute time stamp when creating certificates between DNSSEC servers and clients.

By rejecting the null hypothesis, the alternative hypothesis to be accepted. There is a difference between the two time synchronization methods when securing DNSSEC. Therefore, the problem this research investigated was whether using NTP affects DNSSEC client security performance.

## Restatement of the Research Purpose

The purpose of this research was to evaluate a DNSSEC client's ability to validate a name resolution response and determine the significance of using NTP to improve the ability to detect attacks on DNSSEC certificate authentication and verification when an absolute time stamp was used. By default, DNSSEC servers use the Unix epoch time stamp for certificates. The Unix epoch time stamp is a relative time stamp. DNSSEC clients should be able to validate the resolution response from their stub resolvers.

## Discussion of Research Findings

Cochran (1963) suggests a minimum sample size of 385 iterations for a large population. The first effort at data gathering did test 385 iterations for both Unix epoch and NTP time stamps. At 385 iterations, the p-value for the two proportions test equaled 0.174 which is greater than $\alpha = 0.05$. At the 385 iterations, the null hypothesis could not be rejected. To ensure an accurate representation of the population, the sample size was increased to 800. For an 800 iteration sampling within a 48 hour period, the p-value for the two proportions test equaled 0.00

which is less than $\alpha = 0.05$. At 800 iterations, the null hypothesis can be rejected. Reasoning suggests that there is a point between 385 and 800 iterations where the p-value for the two proportions test just approaches zero.

With a greater sample size of 800, two separate statistical techniques demonstrated that there is a difference in DNSSEC client security when using an absolute time stamp. A smaller sample size was not enough to reject the null hypothesis and conclude that there is a difference when using an absolute time stamp.

Worthy of notice is that one of the original research questions investigated whether a corrupted hash (generated between the DNSSEC server ZSK and the DNSSEC client's KSK) has an influence on DNSSEC client behavior. Upon testing, the DNSSEC/TLSA Validator plug-in used with Firefox was able to detect that the response certificate had been altered, with every iteration using both Unix epoch time and NTP absolute time. There was no variance in its performance. However, even though the DNSSEC client detected the tainted certificate, there were iterations where the DNSSEC client still opened a spoofed web site, unsuccessful at opening the target URL occurrences the data sampling.

## Implications

Name resolution is a part of the Internet counted on to work seamlessly. Name resolution was never built with security features. DNSSEC retrofits some security for name resolution, but there are name resolution vulnerabilities for which Internet users are unaware. To better secure Internet use, DNSSEC encrypts a major Internet service using PKI making the Internet safer to use.

The null hypothesis in this study was rejected, indicating that there is a difference between using the Unix epoch relative time and the NTP absolute time in certificate time stamps.

To mitigate the risk of MiTM attacks, DNSSEC administrators should use the NTP daemon to provide an absolute time stamp to certificates used to communicate with Internet users.

## Recommendations

Further research should be done to determine the sampling size where the two proportions test approaches zero. Also, additional research should be done at iterations significantly great than 800 samples to determine if the p-value increases with larger sampling sizes. It is possible that the p-value for the two proportions test results will appear vase-like on a graph, showing that NTP use in the time stamp becomes more significant as the sampling size approaches the actual population size.

DNS is subject to many vulnerabilities, including the cache poisoning vulnerability disclosed by Dan Kaminsky (2008). Domain name administrators should join a chain-of-trust for the TLD in their registered domain using DNSSEC. The tampering of certificates for DNSSEC name resolution responses is just one vulnerability. To improve the efficacy of DNSSEC, it is recommended that administrators use the NTP daemon to provide an absolute time to the DNSSEC server. As DNSSEC implementation world-wide is still new, further research should be done to investigate other DNSSEC vulnerabilities discussed in the literature.

## Summary

The 2014 hacking of Sony Pictures Entertainment, Target, and Home Depot leads one to conclude that we are in the midst of a new cold war over the Internet. The Internet of Things justifies a security-conscious awareness.

A review of the literature reveals that Internet Privacy Concerns (IPCs) derive from the premise of personal privacy which has at its foundation, human dignity and social contract theory. Concerns about securing privacy in an environment of prolific Internet-capable devices

are growing. Name resolution is an integral part of using the Internet and yet, DNS is vulnerable to several kinds of attacks capable of interfering with common Internet use. DNSSEC was designed to improve DNS security by establishing a chain-of-trust between the SOA and the Internet browser. Despite improvements in DNS security, DNSSEC still has several vulnerabilities cited in the literature that are unique to PKI implementation, from key management to buffer overruns.

This study used quantitative research methods on large population samples to determine the influence of NTP on the DNSSEC protocol. Both a two-proportion and Fisher's exact test were used to analyze the data. Both statistical techniques produced the same results.

The results from the research determined that there is a statistically significant difference between using a NTP absolute time stamp in the public certificate hash of the DNSSEC name resolution response versus using Unix epoch time. There are several recommendations that were made from this study for future research on DNSSEC implementation.

# REFERENCES

"DNSSEC/TLSA Validator". (2011). DNSSEC/TLSA Validator 2.2.0.1. Retrieved January 17, 2015, from https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/

"Lawsuits against Sony Pictures". (2014). Lawsuits against Sony Pictures could test employer responsibility for data breaches. Retrieved from https://ezproxy.indstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsnbk&AN=15257307E1460930&site=eds-live&scope=site

"Massive Cyber Breach at Sony". (2014, December 12). New Allegations against Bill Cosby; Massive Cyber Breach at Sony; Flooding in San Francisco, *CNN Newsroom*. Retrieved from https://ezproxy.indstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsggo&AN=edsgcl.393267180&site=eds-live&scope=site

Ahmad, D. (2008). Two Years of Broken Crypto: Debian's Dress Rehearsal for a Global PKI Compromise. *IEEE Security and Privacy, 6*(5), 70-73. doi: 10.1109/MSP.2008.131

Allen, A. L. (2013). An Ethical Durty to Protect One's Own Information Privacy? (Vol. 64): University of Alabama Alabama Law Review.

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues, 33*(3), 66.

Anderson, S. (2012). *Research Project Learning*. Utah Valley University. Evernote shared notes.

Arends, R. (2005). RFC 4035: Protocol Modifications for the DNS Security Extensions. *Request for Comments.* Retrieved January 19, 2015, from http://www.ietf.org/rfc/rfc4035.txt

Ariyapperuma, S., & Mitchell, C. J. (2007, April). *Security vulnerabilities in DNS and DNSSEC.* Paper presented at the Second International Conference on Availability, Reliability and Security (ARES'07), Vienna University of Technology, Austria.

Ateniese, G., & Mangard, S. (2001, November 5-8). *A new approach to DNS security (DNSSEC).* Paper presented at the 8th ACM conference on Computer and Communications Security (CCS '01), Philadelphia, PA.

Atkins, D., & Austeine, R. (2004). RFC 383: Threat Analysis of the Domain Name System (DNS). *Requests for Comments.* Retrieved November 14, 2010, from http://www.ietf.org/rfc/rfc3833.txt

Basu, A., & Muylle, S. (2003). Authentication in e-commerce. *Communications of the ACM, 46*(12), 159-166. doi: 10.1145/953460.953496

Bedi, S. (2005). Repudiating Morals Legislation: Rendering the Constitutional Right to Privacy Obsolete. *Cleveland State Law Review, 53*(447).

Berghel, H. (2001). The Code Red Worm. *Communications of the ACM, 44*(12), 15-19. doi: 10.1145/501317.501328

Bernabe, A. (2012). Giving Credit Where Credit is Due: A Comment on the Theoretical Foundation and Historical Origin of the Tort Remedy for Invasion of Privacy. *The John Marshal Journal of Computer & Information Law, 29*(493).

Bernstein, D. J. (2006, April 24-26). *Curve2551: new Diffie-Hellman speed records.* Paper presented at the PKC 2006, 9th international conference on theory and practice in public-key cryptography, New York, NY.

Bezanson, R. P. (1992). The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990. *California Law Review, 80*(1133).

Bojanova, I., Hurlburt, G., & Voas, J. (2014). Imagineering an Internet of Anything. *Computer, 47*(6), 72-77. doi: 10.1109/MC.2014.150

Botan, C. (1996). Communication work and electronic surveillance: A model for predicting panoptic effects. *Communication Monographs, 63*(4), 293.

Brandeis, L. D., & Strum, P. (1995). *Brandeis on Democracy*. Lawrence, KS: University Press of Kansas.

Bruin, B. D. (2010). The Liberal Value of Privacy. *Law and Philosophy, 29*(5), 505-534. doi: 10.2307/40926328

Cagalaban, G., & Kim, S. (2011). *Towards a Secure Patient Inforation Access Control in Ubiquitous Healthcare Systems using Identity-based Signcryption*. Paper presented at the 13th International Conference on Advanced Communication Technology (ICACT 2011), Phoenix Park, Republic of Korea.

Capers, I. B. (2013). Crime, Surveillance, and Communities. *Fordham Urban Law Journal, 40*, 959.

Cerf, V. G. (2014). Unfinished Business. *Internet Computing, IEEE, 18*(1), 88. doi: 10.1109/MIC.2014.18

Chen, Guo, S., Duan, R., & Wang, S. (2009). *Security Analysis on Mutual Authentication against Man-in-the-Middle Attack*. Paper presented at the The 1st International Conference on Information Science and Engineering (ICISE2009), Nanjing, China

Chen, B. M., Chen, X., & Chen, Z. (2011). *A Collaborative Network Security Management System in Metropolitan Area Network*. Paper presented at the Third International Conference on Communications and Mobile Computing, Qingdaq, China.

Chen, J. K. (2012). Google Public DNS: 70 billion requests a day and counting. Retrieved from http://googleblog.blogspot.com/2012/02/google-public-dns-70-billion-requests.html

Citron, D. K. (2010). Mainstreaming Privacy Torts. *California Law Review, 98*(6), 1805-1852.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Commun. ACM, 42*(2), 60-67. doi: 10.1145/293411.293475

Cochran, W. G. (1963). *Sampling Techniques* (2nd ed.). Hoboken, NJ: John Wiley and Sons, Inc.

Cohen, J. (2002). *Regulating Intimacy: A new Legal Paradigm*. Princeton, NJ: Princeton University Press.

Corlett, J. A. (2002). The Nature and Value of the Moral Right to Privacy. *Public Affairs Quarterly, 16*(4), 329-350. doi: 10.2307/40441333

Crossman, G. (2008). Nothing to hide, nothing to fear? *International Review of Law, Computers & Technology, 22*(1/2), 115-118. doi: 10.1080/13600860801925003

Cubrilovic, N. (2008). Dot Org First TLD To Implement DNSSEC. Retrieved September 21, 2008, from http://www.techcrunchit.com/2008/07/21/dot-org-first-tld-to-implement-dnssec/

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues, 59*(2), 323-342. doi: 10.1111/1540-4560.00067

D'Urso, S. C. (2006). Who's Watching Us at Work? Toward a Structural–Perceptual Model of Electronic Monitoring and Surveillance in Organizations. *Communication Theory, 16*(3), 281-303. doi: 10.1111/j.1468-2885.2006.00271.x

Decasper, D., & Plattner, B. (1998). *DAN: distributed code caching for active networks*. Paper presented at the Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '98), San Francicsco, CA.

Definition - What is VoIP? (2008). Retrieved October 26, 2008, from http://searchunifiedcommunications.techtarget.com/sDefinition/0,,sid186_gci214148,00.html

Dijk, M. v., Rhodes, J., Sarmenta, L., & Devadas, S. (2007, November 2). *Offline untrusted storage with immediate detection of forking and replay attacks.* Paper presented at the Workshop on Scalable Trusted Computing (STC '07), Alexandria, VA.

DNS vulnerable to cache poisoning. (2008). Multiple DNS implementations vulnerable to cache poisoning. Retrieved February 13, 2015, from http://www.kb.cert.org/vuls/id/800113

Doyal, L. (1997). Human Need And The Right of Patients to Privacy. *Journal of Contemporary Health Law & Policy, 14*(1).

Eastlake, D. I. (1999). RFC 2535: Domain Name System Security Extensions. Retrieved November 11, 2008, from http://www.ietf.org/rfc/rfc2535.txt

Eastlake, D. I., & Laufman, C. (1997). RFC 2065: Domain Name System Security Extensions. Retrieved November 5, 2009, from http://www.ietf.org/rfc/rfc2065.txt

Edge, J. (2009). DNSCurve: an alternative to DNSSEC. from http://lwn.net/Articles/340528/

Ely, J. H. (1973). The Wages of Crying Wolf: A Comment on Roe v. Wade. *The Yale Law Journal, 82*(5), 920-949.

Fairfield, P. (1999). Democracy's Discontent: America in Search of a Public Philosophy. *Social Theory & Practice, 25*(1), 165-167.

Fang, F. (2007). Reengineering the internet for better security*, 40,* 40-44.

Fisher, R. A. (1922). On the interpretation of $X^2$ from contingency tables, and the calculation of P. *Journal of the Royal Statistical Society, 85*(1), 87-94. doi: 10.2307/2340521

Fried, C. (1968). Privacy. *Yale Law Journal, 77*(3), 475-493.

Friedlander, A., Mankin, A., Maughan, W. D., & Crocker, S. D. (2007). DNSSEC: a protocol toward securing the internet infrastructure. *Communications of the ACM, 50*(6), 44-50.

Garretson, C. (2009). Security guru pushes DNS patching. *Network World, 26*(8), 32-32.

Garrow, D. J. (2011). The Legal Legacy of Griswold v. Connecticut. *Human Rights, 38*(2), 26-25.

Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., Boneh, D., & Shmatikov, V. (2012). *The most dangerous code in the world: validating SSL certificates in non-browser software*. Paper presented at the Proceedings of the 2012 ACM conference on Computer and communications security, Raleigh, North Carolina, USA.

Gowsikhaa, D., Manjunath, M., & Abirami, S. (2012). Suspicious Human Activity Detection from Surveillance Videos. *International Journal on Internet & Distributed Computing Systems, 2*(2), 141-148.

Guette, G. (2009). Automating trusted key rollover in DNSSEC. *Journal of Computer Security, 17*(6), 839-854. doi: 10.3233/JCS-2009-0343

Hanson-Smith, E. (1978). Austine's Confessions: The Concrete Referent. *Philosophy and Literature, 2*(2), 176-189. doi: 10.1353/phl.1978.0032

Herzberg, A., & Jbara, A. (2008). Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks. *ACM Transactions on Internet Technology (TOIT), 8*(4).

Herzberg, A., & Shulman, H. (2013, October 14-16). *Fragmentation Considered Poisonous, or: One-domain-to-rule-them-all.org.* Paper presented at the Communications and Network Security (CNS), 2013 IEEE Conference on.

Inness, J. (1992). *Privacy, Intimacy, and Isolation*. New York, NY: Oxford University Press.

IP Spoofing. (2008). Retrieved October 26, 2008, from http://www.webopedia.com/TERM/I/IP_spoofing.html

Israel, G. D. (2009). Determining Sample Size. *Agricultural Education and Communication Program Evaluation*. http://edis.ifas.ufl.edu/pd006

Jacobs, H. (1995). Brandeis on Democracy (Philippa Strum, ed.). *American Spectator - Bloomington-, 28*(4), 62-63.

Johnson, D. G., & Miller, K. W. (2009). *Computer Ethics: Analyzing Information Technology* (4th ed.). Upper Saddle River, NJ: Prentice Hall.

Kalafut, A., & Gupta, M. (2009, 14-18 June). *Pollution Resilience for DNS Resolvers.* Paper presented at the IEEE International Conference on Communications, 2009, Dresden, Germany.

Kaminsky, D. (2008, August 2). *It's The End Of The Cache As We Know It.* Paper presented at the Black Hat USA 2008, Las Vegas, NV.

Kant, I., & Kroeger, A. E. (1882). Anthropology of Immanuel Kant. *The Journal of Speculative Philosophy, 16*(1), 47-52. doi: 10.2307/25667890

Karimi, K., & Hauser, C. (2013). *Internet United-and-Conquer architecture.* Paper presented at the International Conference for Internet Technology and Secured Transactions (ICITST), 2013 8th, London, UK.

Kasper, D. V. S. (2005). The Evolution (Or Devolution) of Privacy. *Sociological Forum, 20*(1), 69-92. doi: 10.2307/4540882

Kato Ku, A. (2005). Talk is Cheap, But a Picture is Worth a Thousands Words: Privacy Rights in the Era of Camera Phone Technology. *Santa Clara Law Review, 45*(679).

Keefe, A. J. (1980). Were Warren and Brandeis all wrong? *American Bar Association Journal, 66*(6), 795.

Keown, J. (2012). *Sir Ian Kennedy and the value of life: building on Glanville Williams' shaky foundations?* : Oxford University Press.

Kim, H.-C., Lee, H.-W., Lee, K.-S., & Jun, M.-S. (2008). *A Design of One-Time Password Mechanism using Public Key Infrastructure*. Paper presented at the 2008 Fourth International Conference on Networked Computing and Advanced Information Management, Gyeongju, Korea.

Kurman, H. (2014). Conversations management should not have via e-mail. *Supervision, 75*(8), 12-13.

Lamb, R. (2015). DNSSEC Deployment Statistics For TLDs. Retrieved March 29, 2015, from http://rick.eng.br/dnssecstat/

Leino-Kilpi, H., Välimäki, M., Dassen, T., Gasull, M., Lemonidou, C., Schopp, A., . . . Kaljonen, A. (2003). Perceptions of autonomy, privacy and informed consent in the care of elderly people in five European countries: general overview. *Nursing Ethics, 10*(1), 18-27. doi: 10.1191/0969733003ne571oa

Li, J., Chen, X., Li, M., Li, J., Lee, P. P. C., & Lou, W. (2014). Secure Deduplication with Efficient and Reliable Convergent Key Management. *IEEE Transactions on Parallel & Distributed Systems, 25*(6), 1615-1625. doi: 10.1109/TPDS.2013.284

Lin, Y.-B., & Tsai, M.-H. (2007). Eavesdropping Through Mobile Phone. *IEEE Transactions on Vehicular Technology, 56*(6), 3596-3600. doi: 10.1109/TVT.2007.901060

Liu, B., & Lu, H. (2009). *A Peer-to-Peer Framework for Accelerating Trust Establishment*. Paper presented at the International Conference on Multimedia Information Networking and Security (MINES '09), Hubei, China.

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

Liu, V., Caelli, W., Foo, E., & Russell, S. (2004). *Visually sealed and digitally signed documents*. Paper presented at the Australasian conference on Computer science, Dunedin, New Zealand.

Long, C. (2013, February 20). NYPD, Microsoft Create Crime-Fighting 'Domain Awareness' Tech System, *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/02/20/nypd-microsoft-domain-awareness-crime-fighting-tech_n_2727506.html

Mantoro, T., Norhanipah, S. A., & Bidin, A. F. (2011, 7-9 April 2011). *An implementation on Domain Name System security extensions framework for the support of IPv6 environment.* Paper presented at the Multimedia Computing and Systems (ICMCS), 2011 International Conference on.

Margalit, A. (2001). Privacy in the Decent Society. *Social Research, 68*(1), 255-268. doi: 10.2307/40971450

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*(2), 243.

Martin, K. E. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. *Journal of Business Ethics, 111*(4), 519-539. doi: 10.2307/23324816

Massé, D. (2013). More Than 30B Devices will Connect to the Internet of Everything in 2020. *Microwave Journal, 56*(6), 55-55.

Massey, D., Mankin, A., Lewis, E., Russ, M., & Gudmundsson, O. (2001). *Public Key Validation for the DNS Security Extensions*. Paper presented at the DARPA Information Survivability Conference and Exposition (DISCEX II'01), Anaheim, CA.

McCloskey, H. J. (1980). Privacy and the Right to Privacy. *Philosophy, 55*(211), 17-38. doi: 10.2307/3750973

McHale, J. V., & Fox, M. (1996). *Health Care Law: Text and Materials* (2nd ed.). London: Thomson-Sweet & Maxwell.

McLean, D. (1995). *Privacy and Its Invasion*. Santa Barbara, CA: ABC-CLIO, Inc.

Michaelson, G. (2010). DNS Resolvers and DNSSEC: Roll Over and Die? Retrieved from http://www.circleid.com/posts/dns_resolvers_and_dnssec_roll_over_and_die/

Mockapetris, P. (1983a). RFC 882: Domain Names - Concepts and Facilities. *Requests for Comments*. Retrieved October 29, 2009, from http://www.faqs.org/rfcs/rfc882.html

Mockapetris, P. (1983b). RFC 883: Domain Names - Implementation and Specification. *Requests for Comments*. Retrieved October 29, 2009, from http://www.faqs.org/rfcs/rfc883.html

Mockapetris, P. V. (2006). Telephony's Next Act. *IEEE Spectrum,* (April). http://www.spectrum.ieee.org/apr06/3204

Moor, J. H. (1997). Towards a theory of privacy in the information age. *SIGCAS Comput. Soc., 27*(3), 27-32. doi: 10.1145/270858.270866

Mosher, D., Nagi, I., Gallo, N., Smith, J., McElhaney, L., & Lye, L. (2014). In 'Domain Awareness,' Detractors See Another NSA. In M. Kaste (Ed.), *All Things Considered*: National Public Radio.

Mutter, A. D. (2014). Get Ready for the Internet of Everything. *Editor & Publisher, 147*(3), 22-24.

National Strategy to Secure Cyberspace. (2003). *The National Strategy to Secure Cyberspace*. Retrieved from http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

Negley, G. (1966). Philosophical Views on the Value of Privacy. *Law and Contemporary Problems, 31*(2), 319-325. doi: 10.2307/1190674

Nissenbaum, H. (1997). Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behavior, 7*(3), 207.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119-158.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Standford, CA: Standford University Press.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online (Vol. 140, pp. 32-48).

NIST. (2009a). *Recommended Security Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 3*. Gaithersburg, MD.

NIST. (2009b). The Secure Naming Infrastructure Pilot (SNIP). Retrieved November 15, 2009, from http://www.dnsops.gov/

Nixcraft. (2009). *Bind Security: Transaction Signatures (TSIG) Configuration*. http://www.cyberciti.biz/faq/unix-linux-bind-named-configuring-tsig/

NTP Project R&D. (n.d.). NTP: The Network Time Protocol. Retrieved October 19, 2007, from http://www.ntp.org/

Olzak, T. (2006, March). DNS Cache Poisoning: Definition and Prevention Retrieved October 26, 2008, from adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf

Oppliger, R., Rytz, R., & Holderegger, T. (2009). Internet Banking: Client-Side Attacks and Protection Mechanisms. *Computer, 42*(6), 27-33. doi: 10.1109/MC.2009.194

Osterweil, E., Massey, D., McPherson, D., & Zhang, L. (2014). Verifying Keys through Publicity and Communities of Trust: Quantifying Off-Axis Corroboration. *IEEE Transactions on Parallel & Distributed Systems, 25*(2), 283-291. doi: 10.1109/TPDS.2013.168

Osterweil, E., Pappas, V., Massey, D., & Zhang, L. (2007). *Zone State Revocation for DNSSEC*. Paper presented at the ACM SIGCOMM 2007 Workshop on Large-Scale Attack Defense (LSAD), Kyoto, Japan.

Pansa, D., & Chomsiri, T. (2008, November 11-13). *Architecture and Protocols for Secure LAN by Using a Soft Certificate and Cancellation of ARP Protocol* Paper presented at the Third 2008 International Confrence on Convergence and Hybrid Information Technology, Busan, Korea.

Pappas, V., Massey, D., & Zhang, L. (2007, June). *Enhancing DNS Resilience against Denial of Service Attacks.* Paper presented at the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07) Edinburgh, UK

Posner, R. (1978). The Right of Privacy. *Georgia Law Review, 12*, 401.

Post, R. C. (1991). Rereading Warren and Brandeis: Privacy, property, and appropriation. *Case Western Reserve Law Review, 41*(3), 647.

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383.

Qi, F., Tang, Z., & Wang, G. (2008, November 18-21). *Attacks vs. Countermeasures of SSL Protected Trust Model.* Paper presented at the The 9th International Conference for Young Computer Scientists (ICYCS 2008), Zhang Jia Jie, Hunan, China.

Rachaels, J. (1975). Why is Privacy Important? *Philosophy and Public Affairs, 4*(Summer), 323-333.

Rachels, J. (1975). Why is Privacy Important? *Philosophy & Public Affairs, 4*(4), 323-333.

Rafiee, H., & Meinel, C. (2013, 22-24 Aug. 2013). *A Secure, Flexible Framework for DNS Authentication in IPv6 Autoconfiguration.* Paper presented at the Network Computing and Applications (NCA), 2013 12th IEEE International Symposium on.

Rappaport, A. J. (2001). Beyond Personhood and Autonomy: Moral Theory and the Premises of Privacy. *Utah Law Review*(441).

Raymond, E. S. (1996). *The New Hacker's Dictionary*. Cambridge, MA: MIT Press.

Reid, J. (2012, October 2). [MITM and DNSsec unix epoch vs NTP].

Richards, D. A. J. (1989). *Toleration and the Constitution*. Oxford: Oxford University Press.

Rijswijk-Deij, R. v., Sperotto, A., & Pras, A. (2014). *DNSSEC and its potential for DDoS attacks: a comprehensive measurement study*. Paper presented at the Proceedings of the 2014 Conference on Internet Measurement Conference, Vancouver, BC, Canada.

Roman, R. C. J. N. (2011). Key management systems for sensor networks in the context of the Internet of Things. *Computers & Electrical Engineering, 37*(2), 147-159. doi: 10.1016/j.compeleceng.2011.01.009

Rose, S. (2012). *Progress of DNS security deployment in the federal government*. Paper presented at the Proceedings of the 26th international conference on Large Installation System Administration: strategies, tools, and techniques, San Diego, CA.

Samz, D. (2007). Face/Off: The Struggle Between Informed Consent and Patient Welfare in Facial Transplant Surgery. *University of Illinois Journal of Law, Technology & Policy, 2007*(89).

Schoeman, F. D. (1992). *Privacy and Social Freedom*. Cambridge: Cambridge University Press.

Schönwälder, J., Pras, A., & Martin-Flatin, J.-P. (2003). On the Future of Internet Management Technologies. *IEEE Communications Magazine, 41*(10), 90-97.

Schwartz, P. M., & Peifer, K.-N. (2010). Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept? *California Law Review, 98*(6), 1925-1987.

Segal, A. (2013). The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists, 69*(5), 38-45. doi: 10.1177/0096340213501344

Shirky, C. (2014). The Key to Successful Tech Management. *Foreign Affairs, 93*(2), 51-59.

Shue, C. A., & Kalafut, A. J. (2013). Resolvers Revealed: Characterizing DNS Resolvers and their Clients. *ACM Trans. Internet Technol., 12*(4), 1-17. doi: 10.1145/2499926.2499928

Smith, J. A. (2008). Moral Guardians and the Origins of the Right to Privacy. *Journalism & Communication Monographs, 10*(1), 63-110. doi: 10.1177/152263790801000102

Snedecor, G. W., & Cochran, W. G. (1989). *Statistical Methods*: Iowa State University Press.

Solove, D. J. (2003). The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure. *Duke Law Journal, 53*(967).

Steiker, C. S. (Fall 2009). Symposium: Great Dissents in Fourth Amending Cases Sponsored by the National Center for Justice and Rule of Law: Brandeis in Olmstead: "Our Government is the Potent, the Omnipresent Teacher". *Missippi Law Journal, 79*(149).

Stephen, S. J. F. (1967). *Liberty, Equality, Fraternity*. Cambridge: Cambridge University Press.

Taberner, S. (2006). Germans, Jews, and Turks in Maxim Biller's Novel "Esra". *German Quarterly, 79*(2), 234-248. doi: 10.1111/j.1756-1183.2006.tb00041.x

Tivani, H. (2007). Philosophical theories of privacy: Implications ofr an adequate online privacy policy. *Metaphilosophy, 38*(1), 1-22.

Top German court confirms ban. (2007, October 12). Top German court confirms ban on true-life novel, *Agentur*. Retrieved from https://ezproxy.indstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsnbk&AN=11C4278DD41841B0&site=eds-live&scope=site

Tunick, M. (2013). Privacy and Punishment. *Social Theory & Practice, 39*(4), 643-668. doi: 10.5840/soctheorpract201339436

USNO NTP Network Time Servers. (n.d.). Retrieved March 27, 2011, from http://tycho.usno.navy.mil/ntp.html

Uusitalo, I., Catot, J. M., & Loureiro, R. (2009). *Phishing and Countermeasures in Spanish Online Banking.* Paper presented at the Third International Conference on Emerging Security Information, Systems and Technologies, Athens/Glyfada, Greece.

Walker, G. (2014). *Moral Foundations of Constitutional Thought: Current Problems, Augustinian Prospects*. Princeton: Princeton University Press.

Warren, S. V., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.