

An Investigation of the Cyber-Attack Susceptibility of State and Local Government Websites

A thesis
by
Patrick Hill
Submitted to the Graduate School of
Charleston Southern University in fulfillment
of the requirements for the degree of
MASTER OF SCIENCE
April 2021

Major: Computer Science

Computer Science Committee:
Advisor: Yu-Ju Lin, Ph.D.
Sean Hayes, Ph.D.
Paul West, Ph.D.

Contents

<i>ABSTRACT.....</i>	<i>3</i>
<i>CHAPTER 1. OVERVIEW.....</i>	<i>3</i>
<i>CHAPTER 2. BACKGROUND.....</i>	<i>6</i>
<i>CHAPTER 3. PAST RESEARCH.....</i>	<i>11</i>
<i>CHAPTER 4. METHODOLOGY.....</i>	<i>26</i>
<i>CHAPTER 5. RESULTS AND ANALYSIS.....</i>	<i>30</i>
<i>CHAPTER 6. CONCLUSION.....</i>	<i>55</i>
<i>CHAPTER 7. REFERENCES</i>	<i>58</i>

ABSTRACT

While much research exists that examines internet-facing systems, the purpose of this study is to provide an analysis on United States local county government systems in an effort to gauge their overall susceptibility to common cyber threats. The United States are under constant attack by malicious actors seeking to disrupt the American way of life. From an overall national viewpoint, it is important that systems that provide critical data and information to citizens are protected from cyber threats.

By using common IT administration tools, such as NMAP and OpenSSL, we examine over 2939 state and local government websites for the adoption of the latest web security technologies, such as HTTPS, TLS 1.3, HTTP Strict Transport Security (HSTS) and HTTP/2. In addition, we also investigate the remediation of common legacy vulnerabilities such as HeartBleed, FREAK, Drown and POODLE exploits. Finally, we also check each site for the evidence of best practices, such as acquiring a .gov domain, disabling unused and risky ports, using certificates that are not self-signed, expired or from outside the US.

The results of this study will show that there are aspects of our local government, citizen facing websites that are not as resilient to cyber-attack as they should be. This research shows that there is a severe need for greater web security assistance from the US federal government. By surveying local government-owned, citizen-centric systems, we can better understand the overall rigidity of our nation's cyber framework and its ability to withstand cyber-attacks and malicious manipulation. In the next section, this study will provide a brief and more detailed introduction which further explains the importance of this research.

CHAPTER 1. OVERVIEW

In this paper, we examine an overlooked component to the nation's critical infrastructure, local governments. Local governments make up the national fabric that links services, citizens, states and the nation together. In this study we present a more holistic view of our nations cyber posture by analyzing local county government websites for their ability to resist legacy exploits, their adoption of emerging technologies and their implementation of best practices. Research on internet vulnerabilities and the adoption of new technologies, typically focuses on the internet as a whole, but I am narrowing the scope and focusing solely on local government websites.

1.1 INTRODUCTION

Our research, "An Investigation of the Cyber-Attack Susceptibility of State and Local Government Websites," will examine 2939 public-facing, state and local government websites to determine cyber-threat susceptibility. Critical infrastructure is those assets, systems, and networks that underpin American society. State and local websites are a significant part of critical infrastructure and are in constant danger of malicious manipulation. In times of emergency, such as with Covid-19, citizens look to their local government websites for information, guidance, and advisement (Prall, 2015). Our research shows that many state and local government websites, a vital component of the nation's critical infrastructure, are not secure. While the national Cybersecurity & Infrastructure Security Agency offers cyber hygiene services for organizations that request it, we argue that our government should be more proactive and engage our local governments with assistance securing their websites from malicious manipulation (Cyber Hygiene Services | CISA, 2020). Municipal governments are those entities defined as cities, towns, boroughs, and townships that are organized around a population center. Municipalities generally take responsibility for parks and recreation services, police and fire departments, housing services, emergency medical services, municipal courts, transportation services, and public works (state-

Local-Government, 2020). The United States are under constant attack by malicious actors seeking to disrupt the American way of life and citizen services are a prime target (Dwoskin & Timberg, 2018).

Risk increases when sharing is inconsistent, fragmented, or non-existent. In the spirit of sharing, this study expects to raise awareness of the state, and local county government website's security status. This research intends to be used as a tool to demonstrate the need for more proactive federal assistance and to inform internal government site owners and partners of the potential risks discovered in citizen facing state and local websites. Managing the looming threats to our nation's cyber-critical systems requires understanding, detection, identification, and collaboration.

This analysis divides the state and local website survey into three sections: Legacy Exploits, Best Practices, and New Technology Adoption. The Legacy Exploits portion of the research, examines a sites remediation of common, well known vulnerabilities such as POODLE, DROWN, FREAK, SWEET32 and Heartbleed exploits. These exploits are easily remediated with patching and their presence would indicate that a website has been neglected. The Best Practices portion of the research, examines top-level domain registration, use of properly configured US based certificates, HTTPS adoption, highest TLS version supported, and risky ports closed. Failure to implement best practices could be an indicator that a website is poorly maintained. The Emerging Technologies portion of this research examines the adoption of new technologies such as HTTPS, Extended Validation certificates, TLS 1.3 and HTTP 2. Utilizing these new technologies would indicate that a site has been given proper care. In addition, we also examine a county's population size, state, and region location, to determine what role these factors may play in a website's resiliency to cyber-attack.

In the next section, this paper will discuss the background leading to the need for this study. Next, the paper will provide a literature review with findings that will outline the past research, its importance, and how it applies to websites. In addition, the findings will present the results of this study, and finally, this research will conclude with a summary of the research and its importance to local governments.

CHAPTER 2. BACKGROUND

In this chapter, we focus on the need for this research. We start the chapter outlining what constitutes a secure local government website. Next, we discuss the call to action by the U.S. government to focus on improving the national cyber security infrastructure. Then, we focus on some of the threats that have been observed within some of our nations citizen centric computing systems. Finally, we close out the chapter with why the call to action and the malicious attacks against our national local government websites pose a serious risk to our national stability.

2.1 ASPECTS OF A SECURE STATE AND LOCAL WEBSITE

Before we can begin discussing the background provided in this research, it is important to understand what a secured website is. A secured government state and local website utilizes the latest technologies like TLS 1.3, a properly configured E.V. (Extended Validation) Certificate, patched to mitigate known vulnerabilities, uses HSTS, uses a C.A. in the U.S., and has a .gov domain registration. In addition, it includes disabled and unused ports, such as port 80, when HTTPS is used. Also, the website should support HTTP/2. This research is vital because misinformation and deception can instigate civil disorder. A primary source of citizen information is their local government website. If malicious actors can alter or manipulate our local government websites, then they can manipulate the population.

2.2 CALL TO ACTION

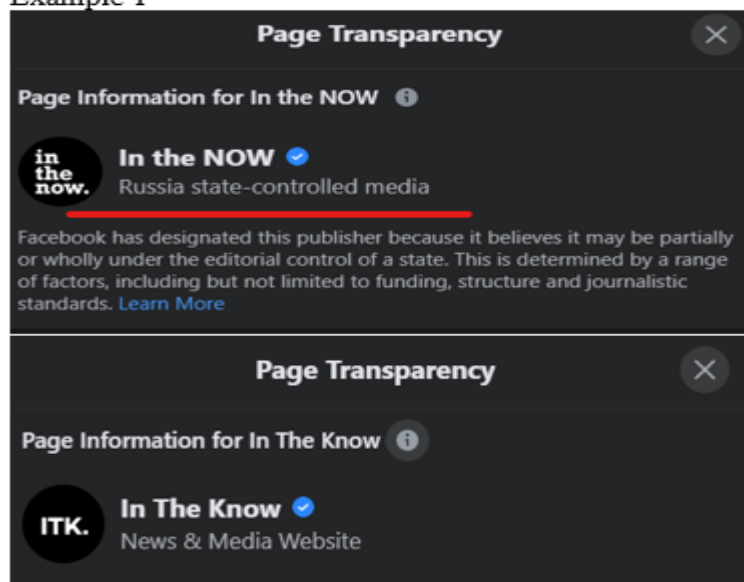
In 2010 the U.S. government surveyed the cyber landscape and began to take significant steps to improve our resiliency to cyber-attacks. In February 2013, the President issued the Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, which explicitly calls for an update to the Nation's Infrastructure Plan. In addition, Executive Order 13636: Improving Critical Infrastructure Cybersecurity supplemented PPD-21 by developing, promoting, and incentivizing the adoption of cybersecurity practices and using existing regulation to promote cybersecurity (Presidential Policy Directive -- Critical Infrastructure Security And, 2013).

2.3 MALICIOUS MANIPULATION

As state and local websites are a crucial tool for citizens, many hacker groups, such as the Russian Internet Alliance or the Iranian Enemies of the People (EOTP), have sought to disrupt citizens' trust and confidence in their governments by targeting state and county webpages (Lohrmann, 2020). Malicious actors will try to gain access to a state or local county government webpage by exploiting unpatched vulnerabilities, misconfigured ports, or weak encryption and use the compromised web server as a launchpad to a more aggressive cyber campaign. Most cyber-terrorist campaigns intend to disrupt citizen trust and confidence in their governments and create civil unrest. Example 1 shows two similar Facebook pages, 'In the Know' and 'In the Now.'

Both sites share the same look, 'feel,' and similar content, yet 'In the Now' displays content containing messages against government-established institutions. If we examine the 'Page

Example 1



Transparency section within Facebook, we can see that 'In the Now' is controlled by the Russian media.

Recently, cybercrime susceptibility has gained increased attention by the U.S. Government due to the impact of state-sponsored hacktivism, hardware\software shipped with spyware, compelled certificates issued for Internet interception, and exploited zero-day exploits (Mazarr, 2019). Local governments form our national fabric and their public-facing websites are the front-line for delivering official information and services to citizens. Attacks targeting these websites can cause widespread panic, citizen instability and disrupt our economy. In addition, malicious actors can use compromises to steal citizen credentials and sensitive citizen data. Public-facing website defacements typically involve a cyber threat actor compromising the website or its associated content management system, allowing the actor to upload images to the site's landing page. In situations where such public-facing websites relate to the state and county government (e.g., the website of a county board of elections), defacements could cast doubt on the websites' information security and legitimacy. As we have seen with the Capitol riots in D.C., citizens can easily be coerced into civil disorder (Mazarr, 2019).

If cyber actors could successfully change a state or local government agency website, the underlying data and internal systems would remain uncompromised, yet the website could easily convey false information or show disturbing images. Example 2 shows the Town of Hilton Head had experienced a breach of their webserver on 10/4/2020, resulting in the below defacement shared with me by the State Law Enforcement Division (SLED). Attacks such as these are not always made public.

Example 2



As state and county websites are considered critical information infrastructures by homeland security, this research investigates their susceptibility to common cyber-attacks, the adoption of web security policies such as HTTP Strict Transport Security (HSTS), certificate type, and TLS version supported (Information Technology Sector | CISA, 2021). In addition, this research will also examine state statutes on data security due to the critical role Government policies play in cybersecurity. This research will examine the public external-facing local government agency websites across the U.S. to probe into the concept of our nation's overall cyber threat susceptibility and security. While the literature has been published demonstrating the cause and effect of various exploits, little has been written to show how susceptible our nation's citizen-facing cyberinfrastructure is to these exploits. The Past Research section shows that the current literature on cyber susceptibility focuses on the internet as a whole but not specifically state and

county government websites. This study will apply current research literature on vulnerabilities and test our nation's local government web infrastructure.

CHAPTER 3. PAST RESEARCH

In this chapter, we will provide detailed information on the past research that has been performed. The past research will examine many insecurities in websites and web communications and how web administrations can mitigate them. It is essential to understand past research and how it applies to web systems. We can use this past research and apply it to an analysis of state and county government websites only. Chapter 3 will be divided into 4 sections, Earlier Investigations, Best Practice Research, Emerging Technologies and Chapter 3 summary.

Earlier Investigations will discuss several examples of the early research performed on malicious activity that was perpetrated against local governments, namely election offices. Next, Best Practice Research will discuss the importance of adequate site administration activities, such as HTTPS, TLS adoption, disabling unneeded services, and .gov domain registration. The Legacy Exploit section will discuss the POODLE, DROWN, SWEET32, FREAK, and Heartbleed exploits that will be examined in the research. Finally, the Summary Section will provide a brief review of the chapter.

3.1 EARLIER INVESTIGATIONS

Much research has been done documenting the vulnerabilities and exploits in web systems. Yet, no recent study has been discovered that analyzes only U.S. state and county government web domains' susceptibility to cyber threats, alone. Many state and county government websites are not associated with a valid .gov domain and therefore have not gone through the vetting process associated with obtaining a .gov domain. Such few County's use a .gov domain for their website that an attacker can easily spoof a local government site and convey false information to citizens. Minnesota and Texas have the most significant number of county sites that do not use the .gov

domain (Vijayan, 2018). Poorly secured County websites with a low level of autonomy give attackers a much more realistic opportunity to influence and disrupt citizen activities.

The article “County Election Websites Can Be Easily Spoofed to Spread Misinformation” brings attention to how county government websites in 20 key swing states do not use a .gov domain nor enforce the use of SSL. At the time of the article, Minnesota and Texas have the most significant percentage of non-.gov county government sites, with 95% of their county sites using HTTP (Vijayan, 2018). West Virginia, Texas, and Montana have the most considerable number of county governments not using SSL, which would allow attackers to redirect website visitors to alternate, malicious sites. The article states that lack of consistency in website naming and improper use of SSL certificates pose a much more realistic threat to the election process’s integrity than a physical attack on voting machines. Often, County election sites are the first-place voters go-to for eligibility requirements, voting locations, registration deadlines, and hours. It is feared that simple misinformation campaigns focused on vulnerable gaps at the local level could negatively impact voting results. Poorly secured county websites give attackers a much more realistic opportunity to influence the outcome of elections. Since not all counties use a .gov domain, voters would have difficulty identifying spoofed sites from real ones (Vijayan, 2018).

Inconsistency in website naming and the lack of SSL certificate use make county websites a high-profile target for malicious actors. The .gov top-level domain (TLD) facilitates collaboration among government-to-government, government-to-business, and government-to-citizen entities. The TLD authorizes domain names for bona fide US-based government organizations at the federal, state, and local levels, including federally recognized Indian tribes and Alaskan Native groups, known as native sovereign nations (NSNs). The .gov domain designation makes government services easy to identify on the internet.

There is evidence which reveals that malicious actors are targeting citizen centric services. The hacker group APT28 actively interfered with the 2016 presidential election, with many sites being created to spoof local government sites. The article “Microsoft-says-it-has-found-a-Russian-operation-targeting-us-political-institutions” states that during the 2016 election, a group affiliated with the Russian government created fake versions of six websites with the goal of hacking people that visited these fake websites; some of which were related to public policy and the U.S. Senate (Dwoskin & Timberg, 2018). U.S. officials repeatedly warned that the November elections are a significant focus of malicious interference efforts. APT28, which is sometimes called Strontium or Fancy Bear is a unit under the Russian Military intelligence agency GRU, which specializes in misinformation. APT refers to an advanced persistent threat. Hackers will often send out fake e-mails, directing people to visit sites that appear to be legitimate (Dwoskin & Timberg, 2018).

The prior research has shown that malicious attackers are targeting US citizen servicing systems. In addition, without consistent and uniform site best practices enforced, it becomes increasingly difficult for citizens to recognize and fake or malicious site. The Best Practice section of Chapter 3 will show that adopting proper site administration activities, such as patching and domain name registration, can mitigate many of the threats facing our state and local government websites.

3.2 BEST PRACTICE RESEARCH

In this section of Chapter 3, we will discuss aspects of site administration that help ensure a more secure site configuration. We will discuss registrations to a .gov domain, US based certificate use, certificate handling, and closing unused ports.

Every .gov domain name application is carefully examined to ensure domain names requested will not create misunderstandings about the purpose of domains and their content. The

.gov vetting process's overall goal is to maintain domain name integrity, eligibility is limited to qualified government organizations, and programs for having a managed domain name such as .gov assures citizens that they are accessing an official U.S. government site. General Services Administration (GSA) arbitrates domain name issues and reserves the right to deny domain name requests that do not adequately meet requirements. Title 41 Public Contracts and Property Management in the [Code of Federal Regulations Chapter 102, sub-chapter 173](#) outlines Government requirements for a .gov domain. Domain names must be authorized by the Chief Information Officer (CIO) of the requesting or sponsoring governmental organization. For Federal departments and agencies, the General Services Administration (GSA) will accept authorization from the department or agency's CIO. For independent Federal government agencies, boards, and commissions, GSA will accept authorization from the highest-ranking Information Technology Official. For State and local governments, GSA will accept authorization from appropriate State or local officials (Lohrmann, 2020). On March 10th, 2020 the U.S. began taking notarized signatures for the .gov domain vetting process. Because the U.S. does not require its local governments to have .gov domain registration, official state and local county government websites can be easily impersonated. In addition, the financial requirements to obtain a .gov domain are significantly higher than that of the other domain registrations.

Not only are local governments using non .gov domains, but research shows that many county government sites still use HTTP for their web server communications instead of the more secure HTTPS. HTTPS runs HTTP over Transport Layer Security (TLS), a fundamental security protocol that enables end-to-end encryption and authentication for HTTP connections (Dwoskin & Timberg, 2018). Research into a novel attack on TLS titled "A cross-protocol attack on the TLS protocol," authors Mavrogiannopoulos, et al. show that TLS alone is fallible (Mavrogiannopoulos

et al, 2012). The authors present a cross-platform exploit that shows an attacker can interpret signed explicit elliptic curve Diffie-Hellman (D.H.) key exchange parameters as valid plain parameters that enable the impersonation of a trusted server. The server must support the elliptic curve options for the attack to be successful. Proper configuration of HTTPS sites is essential to improving their cyber-security as HTTPS adoption improves. The paper describes the TLS protocol as an agile protocol that allows peers to negotiate their highest supported protocol version and use a combination of ciphers during each session (Mavrogiannopoulos et al, 2012). The TLS cipher suite determines the symmetric encryption cipher with its operational mode, the key exchange method, and the message authentication algorithm. The TLS downgrade dance is for backward compatibility with legacy servers. During handshake negotiation, a server will attempt to use the highest level of TLS that the client supports. If the handshake fails, a retry will be initiated using the next lowest TLS version. POODLE, Drown, and Freak attacks are all examples of attacks against the TLS stack.

Best practices are those processes that, when carried out, will produce optimal results. In secure website administration, best practices are using HTTPS, frequent software updates, and proper domain name registrations (to improve citizen confidence). By utilizing these best practices, we can ensure that our nation's websites are secure and trustworthy for citizens.

3.3 LEGACY EXPLOITS

In this section of the background research chapter, we will discuss the examined legacy exploits. The Legacy Exploits surveyed by this research are POODLE, DROWN, FREAK, SWEET32, and Heartbleed. These vulnerabilities were specifically chosen because their security exploits are well documented, they are easily mitigated, and extremely effective. We used a

combination of NMAP, OpenSSL, and packet investigation to look for evidence that these exploits have or have not been remediated.

3.3.1 THE POODLE ATTACK

The POODLE (Padding Oracle on Downgraded Legacy Encryption) attack will attempt to intercept the TLS (Transport Layer Security) handshake negotiation to force a weak SSL 3.0 connection. If a POODLE attack against a susceptible state or county website is successful, a malicious actor would have command and control capabilities of the citizen serving system. In the paper, "POODLE Bites: Exploiting the SSL 3.0 Fallback," the authors stress the need for proper TLS and webserver security configuration and the disabling of older legacy support protocols such as SSL 3.0 (Bodo et al., 2014). In the work "SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancement," authors Clark and Oorschot show many of the on-going security flaws with HTTPS as attacks involving fraudulent certificates, SSL stripping attacks, and the lack of HTTPS support (Clark & Oorschot, 2013). Not only do attacks against the TLS stack exist but also attacks against the TCP headers.

3.3.3 THE DROWN ATTACK

The Drown attack (Decrypting RSA with Obsolete and Weakened eNcryption) is like a POODLE attack in that it pushes the server to an obsolete encryption algorithm. DROWN is an attack on an even older protocol version, SSL 2.0. Proper server administration is the key to mitigating this attack; simply disabling support for SSL 2.0 will prevent this vulnerability. Conversely, patching SSL to a later version will also mitigate this attack (Aviram et al., 2016).

3.3.4 THE FREAK ATTACK

The FREAK attack (Factoring RSA Export Keys) occurs when a man-in-the-middle attacker forces a client to use older and weaker encryption. The attacker will be able to break the

encryption and steal sensitive information, including citizen data, or launch an attack by injecting malicious code in the encrypted stream of data. FREAK attacks can be mitigated by patching OpenSSL to the latest version. In the research “A Messy State of the Union: Taming the Composite State Machines of TLS,” the authors used internet-wide scans to estimate that more than alarmingly 25% of HTTPS servers still supported RSA_EXPORT (FREAK attack) (Beurdouche et al., 2017).

3.3.5 THE SWEET32 ATTACK

The SWEET32 attack is an attack on block ciphers that have a block size of 64 bits. These ciphers are vulnerable to a practical collision attack when used in CBC mode. This attack is easily mitigated by deprecating all versions of SSL/TLS protocols that support cipher suites that use 3DES as the symmetric encryption. The DES and Triple DES ciphers, as used in the TLS, SSH, and IPsec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple-DES in CBC mode, aka a “Sweet32” attack.

Older ciphers, such as TLS_RSA_WITH_3DES_EDE_CBC_SHA, lack of forward secrecy, meaning there is no encrypted key exchange. Therefore, if the private RSA key is leaked, all passively captured past data exchanges can be decrypted. In addition, the CBC padding issues are available to attackers because AES-CBC is used in a mac-then-encrypt situation where the padding is removed before the message is authenticated.

3.3.6 THE HEARTBLEED EXPLOIT

Heartbleed is a code flaw in the OpenSSL cryptography library. In the study, “The Matter of Heartbleed”, the authors perform a comprehensive, measurement-based analysis on the vulnerability impact, including tracking the population, monitoring the patching behavior over time, and assessing the HTTPS ecosystem's impact and exposing real attacks (Durumeric et al., 2014). The authors found that 44 of the top 100 Alexa websites remain vulnerable two months after the patch was released. In addition, only 10% of analyzed websites replaced their certificates compared to 73% that patched their site and 14% of those using the same private key (Durumeric et al., 2014), HTTPS is the secure variant of the HTTP protocol on which the web is based. HTTPS provides cryptographic security protections by carrying HTTP messages over the TLS protocol instead of directly over TCP (Transmission Control Protocol). HTTPS websites authenticate using digital certificates as part of the TLS handshake. Web users are shown an invalid certificate warning when their browser cannot validate the identity of the websites they are visiting. Based on this study, no state and local county government websites examined were susceptible to a Heartbleed attack.

While these warnings often appear in benign situations, they can also signal a man-in-the-middle attack. However, many more frequent users are connecting to a legitimate website with erroneous or self-signed certificates. The research performed by Joshua Sunshine, Serge Egelman, Hazim Almuhiemedi, Neha Atri, and Lorrie Faith Cranor in "Crying Wolf: An Empirical Study of SSL Warning Effectiveness" shows that invalid certificate warnings can signal a man-in-the-middle attack or a DNS (Domain Name System) spoofing attack (Sunshine et al., 2009). The authors surveyed 400 Internet users to examine their reactions to understanding website certificate warnings and their effectiveness. Their research showed that the warnings are often by-passed and

that preventing users from making connections to unsafe websites is the safer approach (Sunshine et al., 2009).

POODLE, FREAK, DROWN, SWEET32, and HEARTBLEED vulnerabilities demonstrate the importance of thorough website administration. These vulnerabilities can be easily be mitigated by disabling older, more insecure versions of SSL or by patching servers with the latest code updates. Keeping systems up-to-date with the latest patches, updates and technologies reduces the risk of malicious compromise and protects citizen serving systems integrity.

3.4 EMERGINING TECHNOLOGIES

In this section of the background research, we will discuss HTTP/2, TLS 1.3, HTTP Strict Transport Security and Extended Validation certificates. It is important to adopt new technologies because many advancements in cyber security correct past insecurities.

Browsers enforce additional policies for HTTPS pages, for example, ensuring that HTTPS pages cannot load scripts from non-secure sources. Authors Felt, Barnes, et al. of the paper "Measuring HTTPS Adoption on the Web" attempt to measure the HTTPS adoption rate of the internet (Felt et al., 2017). The authors state the tremendous growth in HTTPS adoption has been positively trending since 2016, with half of the top 100 websites supporting HTTPS. HTTPS provides cryptographic security protections by carrying HTTP messages over TLS instead of directly over TCP. HTTPS works by utilizing public-key cryptography and third-party digital signatures to encrypt and confirm data communications between clients and servers. Communications between the browser and the webserver are not accessible in plaintext to intermediate entities. Intermediate entities cannot make modifications to content sent between the browser and the webserver. The client is assured that the other end of the channel is the one that it

intends to communicate with (Felt et al., 2017). Projects like the "Let's Encrypt," HTTPS only standard and search ranking changes to promote HTTPS are credited with pushing HTTPS adoption rates. Browsers now require HTTPS to unlock and enable certain features. HTTPS is focused on protection against network attackers but does not protect against other types of attacks. However, without HTTPS, the job of attackers becomes much more accessible. Without HTTPS, traffic can be intercepted by an inline adversary, as well as off-path adversaries who are capable of hijacking routes. This inflight manipulation of web page content is one of the significant reasons to abandon HTTP websites.

Nearly all secure web communications take place over HTTPS. HTTPS is based on TLS encrypted transport protocol and supporting key infrastructure of thousands of certificate authorities (C.A.'s) – entities trusted by users' browsers to vouch for a web server's identity. TLS is one of the major secure communication protocols on the internet. It is an agile protocol that allows peers to negotiate their highest supported protocol version and the combination of ciphers used in a session. Not all cipher suites within TLS are strong. The paper "Analysis of the HTTPS Certificate Ecosystem" lists that data is collected by performing 110 Internet-wide scans over 14 months and identify vulnerabilities and user-facing errors that negatively impact the internet ecosystem's overall security (Durumeric et al., 2013). In the paper, the authors investigate the trust relationship between root authorities. The authors analyzed 1832 CA certificates controlled by 683 organizations and found that 80% of the organizations do not have commercial certificate authorities' certificates. The CA's constraints investigated and found that only 7 C.A. (Certificate Authority) certificates use name constraints, and more than 40% of the C.A.'s have no length constraint. The authors identify two sets of miss-issued C.A. certificates. The authors found many problematic security issues within their study, such as a public key compromise that would require

26% of the HTTPS websites to obtain new certificates. They found that half of the trusted leaf certificates contain an inadequately secure 1024 RSA key in their trust chains (Durumeric et al., 2013).

It has been shown that malicious actors can undermine the trustworthiness of the TLS certificates framework. While expired and self-signed certificates can encrypt data, the security alerts displayed will cause citizens to believe the data is untrustworthy. A standard, domain-based validation provides a low-security level, as a man-in-the-middle adversary can impersonate a domain and obtain a trusted validated (DV) certificate for this domain. C.A.s (Certificate Authorities) offer distinct types of certificates to remedy such problems and meet stronger protection demands. The types differ in the way a C.A. conducts the identity validation. Extended Validation (E.V.) certificates are believed to be more secure since a C.A. completing the public key validation is obligated to perform a more detailed validation, sometimes including a face-to-face verification. The extended validation (E.V.) certificates are believed to be the most secure of the certificate offerings because the C.A. must conduct a rigorous identity verification procedure (Szalachowski, 2019).

Content Providers (CP) are servers that host web resources for websites and pose another potential entry point for malicious actors. When a website loads resources from untrusted servers, various undesirable consequences can occur, such as the execution of malicious scripts, malicious content, mining cryptocurrencies, or sending bot-net attacks (Durumeric et al., 2013). In the research work “Re-Architecting the Internet”, the authors state that security in the WWW architecture is based on authenticating the source server and securing the data during transport without considering its content (Feldmann et al., 2009). The traditional assumption is that a page is as secure as the server hosting it. However, modern websites often have a composite structure

where different actors author components of the web page and one logical page contains components collected from disparate servers. Applying a single security policy to a whole page is inadequate. They introduce a novel way of protecting users from web-based malware, which is a new model that uses opportunistic personas to better secure web content by adding integrity and accountability to individual elements. In this paper, the authors present the overall design of the mechanism and details derived from a prototype of the system (Feldmann et al., 2009). Webservers naturally have many attack vectors and by not properly securing the server, risk is amplified.

3.4.1 TRANSPORT LAYER SECURITY 1.3

TLS 1.3 is an important enhancement because it eliminates several vulnerabilities, but our research will show that it is not widely adopted by state and local county government websites. The Transport Layer Security (TLS) Protocol Version 1.3 as of this writing, TLS 1.3 is the latest version of TLS. This new protocol version is almost a complete redesign, with striking differences to previous versions in the protocol and its use of cryptography. In the research “Tracking the deployment of TLS 1.3 on the Web: A story of experimentation and centralization” performed by Holz and Hiller et al., the authors note that just 15 months after standardization, it is used in about 20% of connections they observed. Deployment on popular domains is at 30% and at about 10% across the com/net/org top-level domains (TLDs) (Holz et al., 2020).

TLS 1.3 eliminates the padding in block ciphers. Block ciphers are still accepted, but they must be run in stream mode, creating streams of pseudo-random data of arbitrary length. In addition, encryption and authentication have been combined into a single element. This new type of variant of Authenticated Encryption construction is called Authenticated Encryption with Additional Data (AEAD). Finally, TLS 1.3 only includes the bulk cipher and the hashing algorithm

TLS_AES_256_GCM_SHA384. Separate key exchange and signature algorithms are no longer needed. Also, TLS 1.3 includes just five recommended cipher suites:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

The operational benefits of being able to control both endpoints of a connection are undeniable. HTTP Strict Transport Security (HSTS) is a policy for web security in which a web server can restrict communications only to HTTPS connections from browsers, denying HTTP connections. HSTS helps mitigate man-in-the-middle attacks by preventing clients from downgrading from HTTPS to HTTP. An HTTP request to a website enabled with HSTS will automatically be upgraded to HTTPS. This upgrade to from HTTP to HTTPS will ensure that the communications are encrypted with TLS. Further work into ensuring that TLS is used by browsers has been performed with the development of HTTP/2.

3.4.2 HTTP/2

HTTP/2 is the latest iteration of the HTTP protocol, and provides a significant security advantage, but our research will show that it is not widely adopted among state and local government websites. In the research "Exploring HTTP Header Manipulation In-the-Wild" [16], the authors investigated web page headers' exploitation. Headers are attribute-value pairs that are emended within all HTTP messages. Headers are a critical complement to HTTP; their investigation reveals that 25% of their measured autonomous systems (AS) modify the HTTP headers. Once headers are transmitted across a network, they become vulnerable to manipulation.

Therefore, a secure site should use the most current iteration of HTTP headers, HTTP/2.0, which is currently supported by all major browsers. HTTP2 has many performance enhancements over the HTTP1 standard, but to utilize these improvements, TLS is required. This means that TLS encryption is mandatory for a website to take advantage of HTTP/2's performance advantages (Tyson et al., 2017).

3.4.3 DANGERS OF OPEN PORTS

Apart from the protocol's performance benefits, HTTP/2 improves security by requiring TLS (Wolsing et al., 2019). Open ports on a web server that is internet facing pose a serious risk to the web server itself. Open ports are dangerous to a webserver's security when the port's listening service is misconfigured, unpatched, or vulnerable to exploitation. In addition, malicious services can use open ports to communicate and exfiltrate data without using traditional ports and can add another layer of detection avoidance. Less open ports will reduce the attack surface of the webserver and reduce the overall risk of a breach. Some of the riskiest services to leave open on an internet facing webserver are FTP, SSH, Telnet, SMTP, DNS, SQL, SMB, NetBIOS, and RDP.

In summary, past research has identified various weak points and threats facing the underlying operations of our web structures. Research has shown that HTTPS is important because malicious 3rd parties can intercept network traffic without it. Research has shown that E.V. certificates are designed to prevent phishing attacks and are more secure due to the rigorous C.A. checks that are required to obtain them. In addition, self-signed certificates are problematic due to the errors on the client-side then generate, which leads to citizen distrust. Certificate country of origin is important as well. Relying on certificate authorities based outside the U.S. can lead to the exploitation of the TLS communication channel by foreign powers. Emerging technology, such as HSTS, has demonstrated its importance because it allows a server to specify that it will only accept

HTTPS connections from browsers, preventing man-in-the-middle attacks. User confidence can be increased by applying and implementing a .gov domain to the state and local county government website. Additionally, attacks against the TLS stack are easily mitigated with proper site maintenance and patching. In Chapter 4, we will show the methodology used to collect the data. This data will reveal that many state and county government websites have not corrected known legacy vulnerabilities, nor have they adopted best practices, nor have they implemented emerging security features.

CHAPTER 4. METHODOLOGY

In this section, we will provide the methodology that we used to conduct our research. In the paper "An Investigation of Cyber Autonomy on Government Websites", the authors identify four significant forces that can influence the degree of a local government's autonomy, including HTTPS adoption, website development, outsourcing, and citizens' fear of large-scale surveillance, and user confusion (Hsiao et al, 2019). My study attempts to expand this research and to provide an analysis of local governments in an effort to bring awareness to local government website insecurities and validate their trustworthiness.

Threats and vulnerabilities should be identified and managed in a coordinated and comprehensive way. There is no sole source that maintains the list of local government websites; therefore, we searched for every US county using the google search engine and looked at the top 10 results of every county listed on the Census.gov website. Using this discovery method, we were able to create a dataset of 2939 state and local county government web domains.

According to the United States Census Bureau, there are 3141 counties in the US (US Census Bureau, 2018).

“The United States total includes 3,006 counties; 14 boroughs and 11 census areas in Alaska; the District of Columbia; 64 parishes in Louisiana; Baltimore city, Maryland; St. Louis city, Missouri; that part of Yellowstone National Park in Montana; Carson City, Nevada; and 41 independent cities in Virginia.” - US Census Bureau, 2018

Not every US County has a web site. For example, Rawlins County, Kansas, has a decentralized web presence in which various elected and appointed offices have their own web pages but a

County specific site does not exist. State and county government Facebook pages were not examined as part of this study. In addition, some County web sites are nested under the state with which the county resides. For example, in Connecticut, Litchfield County and Hartford County are subsites of portal.ct.gov, the main state page. In these situations, only the primary domain was surveyed, not the subsites. Some counties utilize the city website for their primary communication. There are some instances where the Census Bureau has logged a major city population, separate from the county, for example Baltimore City and Baltimore County. In these situations, the city site was used as well. Overall, I was able to locate 2939 unique websites via web query.

This research will examine and log 2939 U.S. state and local government websites for HTTPS adoption, HSTS adoption, valid certificates, originating certificate country, and TLD domain designation, highest TLS version and vulnerability status. A combination of custom code and standard-analysis tools were used to gather the data from the state and county government websites. The results of the analysis were then divided into three categories, Legacy Exploits, Best Practices, and Emerging Technologies.

Certificate Country Code, TLS version, Certificate Issuer, Certificate type and Certificate signed\expiration date was collected using the OpenSSL. The OpenSSL command that is loaded by our custom cpp program is **'echo "Q" | openssl s_client -connect <government website> 443'**.

For gathering vulnerability and exploit analysis, open ports, TLS version, and certificate issuer for this research we used the nmap command loaded by our custom cpp program: **'nmap -p 80,443 --script=ssl-enum-ciphers, ssl-cert, ssl-poodle, ssl-heartbleed, sslv2-drown <government website>'**

We use the CURL commands below to collect the HTTP, HTTPS, and HSTS adoption metrics used by state and county government websites.

```

curl_easy_setopt(curl, CURLOPT_URL, http_result);
curl_easy_setopt(curl, CURLOPT_HTTP_VERSION, CURL_HTTP_VERSION_2_0);

curl_easy_setopt(curl, CURLOPT_HEADER, 1);
curl_easy_setopt(curl, CURLOPT_WRITEFUNCTION, WriteCallback);
curl_easy_setopt(curl, CURLOPT_WRITEDATA, &readBuffer);
res = curl_easy_perform(curl);
curl_easy_cleanup(curl);
GitHub link complete code applications used for this research.1

```

Table 1 represents the benchmark scoring for each item investigated for this study. A perfect overall benchmark is 35.

Table 1: Benchmark

Legacy Exploits		
Exploit	Status	Point
SWEET32	Not Vulnerable	3
HeartBleed	Not Vulnerable	3
POODLE	Not Vulnerable	3
DROWN	Not Vulnerable	3
FREAK	Not Vulnerable	3

Best Practices		
Domain Registration	.gov	2
US based certificate	Found	2
US based root certificate	Found	2
HTTPS	Found	2
Highest TLS level supported	TLS 1.2	2
	Not self-signed	2
Certificate Handling	Not expired	2
Port 80 closed when using HTTPS	Closed	2

Emerging Technologies Adopted		
HTTP Strict Transport Security (HSTS)	HSTS Found	1
TLS 1.3	TLS 1.3 Used	1
HTTP2.0 Used	HTTP/2	1
Enhanced Validation Certificate	EV Certificate	1

Perfect Score	35	
----------------------	-----------	--

¹ <https://github.com/patrickjhil01/thesis>.

Finally, county population data for each examined website was extracted from the US Census website. We have placed each state and county government site into categories as classified by the Center for Digital Government (CDG), a national research and advisory institute on information technology policies and best practices in state and local government. The categories are 1,000,000 or more population category, 500,000 – 999,999 population category, 250,000 - 499,999 population category, 150,000-249,999 population category, and the up to '150,000 population' category. Since there are over 2000 county websites in the 'up to 150,000' category, we felt it was best to divide this category into two categories, '1 to 75,000' and '75,001 – 150,000', respectively.

We need a system to better evaluate and rank the vulnerability of our state and county government websites. Therefore, each state and county website will also be given a benchmark based on their analysis for further segmentation and study. A simple scoring method will be applied to each examined state and county websites. A point(s) will be applied to each county website for each positive aspect web security. Table 1 shows a summary of each scoring criteria used in this study.

Our research uses a combination of personnel inquiry and standard I.T. Admin tools such as Nmap, OpenSSL, and curl to catalog the various aspects of susceptibility. Nmap, OpenSSL, and Curl were selected because they are readily available and part of the traditional tools available within a typical I.T. professional's toolbox. In addition, the chosen tools provide little impact on the local governments webserver's functionality and do not hinder the performance of a site. In the next section, we will discuss the findings of this research.

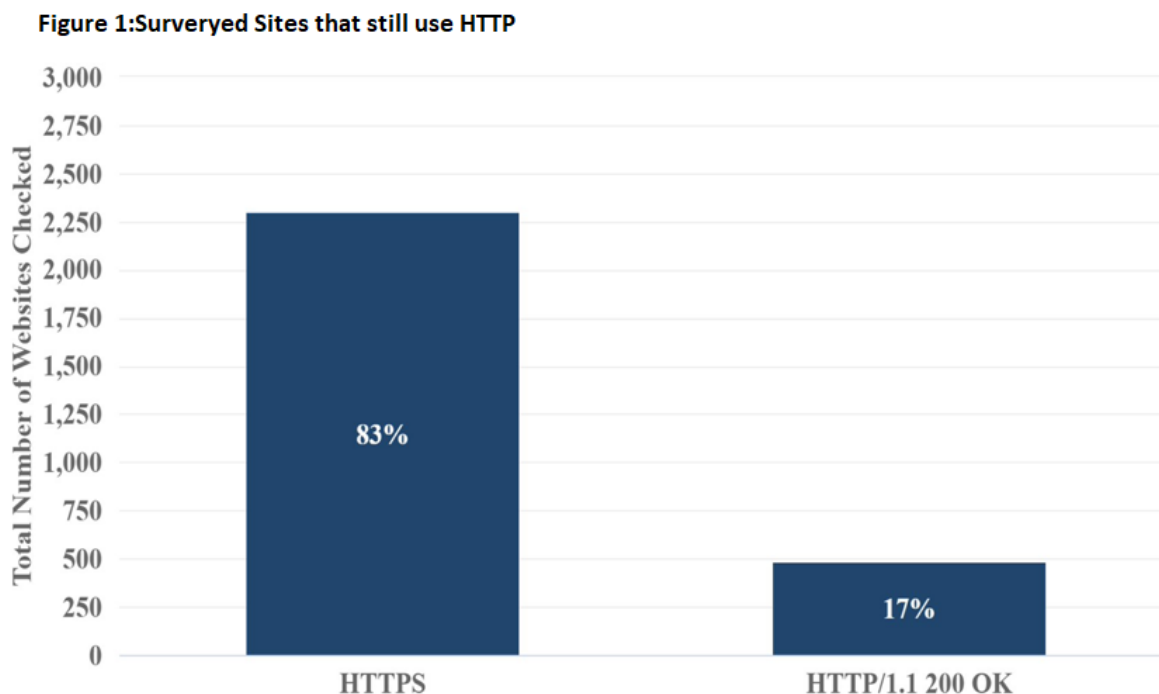
CHAPTER 5. RESULTS AND ANALYSIS

In this chapter, we will present the findings of this research. The result data will be presented in various ways. We will examine each aspect of the data collection and make comparisons between the state, region, and county population. It is important to consider the impact that population plays into a county websites management due to the funding allocated to IT management. First, we will examine the Best Practice Results of our analysis which will include HTTPS adoption, TLD domain registration, certificate handling, service management and TLS level. Next, the Legacy Exploit section will examine the susceptibility of compromise from the POODLE, SWEET32, HeartBleed, FREAK and DROWN vulnerabilities. Finally, the Emerging Technology section, will examine the adoption of new technologies HSTS, HTTP/2, TLS 1.3 and EV Certificates by county websites.

5.1 BEST PRACTICE RESULTS

Best Practices are those process or procedures that are deemed to be the most effective. We have seen that closing unneeded open ports by minimizing services, utilizing a .gov TLD domain, and

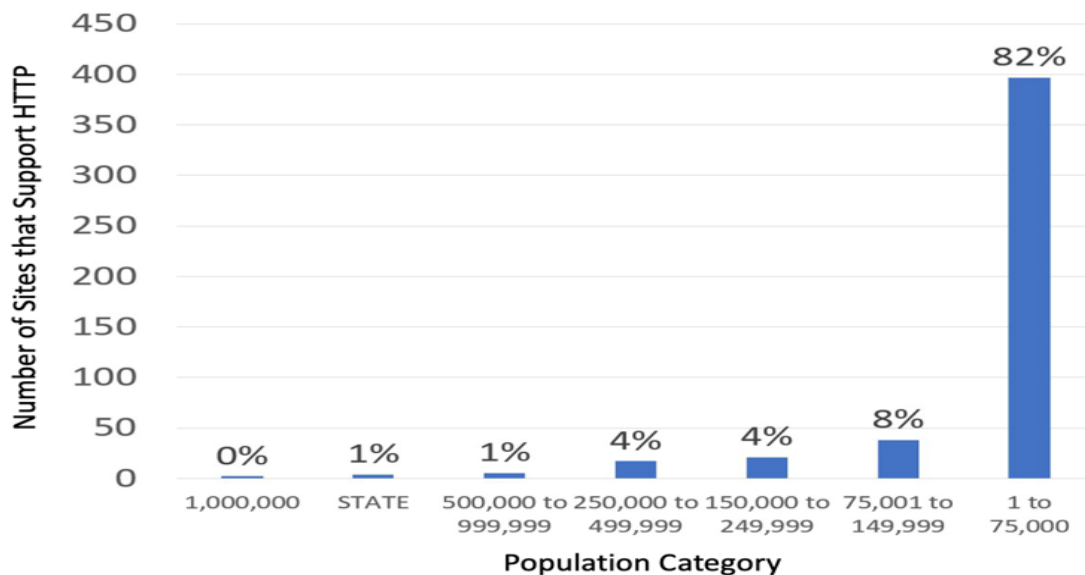
using properly configured security certificates are best practices for a secured government website.



We have indicated in past research that HTTPS is the more secure option for securing web traffic. The results of our analysis reveal that of the state and local county government sites studied, 17% (441) still accepted HTTP connections (Figure 1). This could imply that securing citizen serving web traffic is not a priority for 441 county governments and there may be a lack of understanding on the importance securing data integrity that is used by citizens for information by these counties. In addition, 83% of all state and local county government websites that still accepted HTTP connections were counties in the ‘1 to 75,000’ population category (Figure 2). Due to the number of county sites that support HTTPS that are in the same population category, we do not believe that lack of HTTPS support from these 441 counties is funding related. It is important

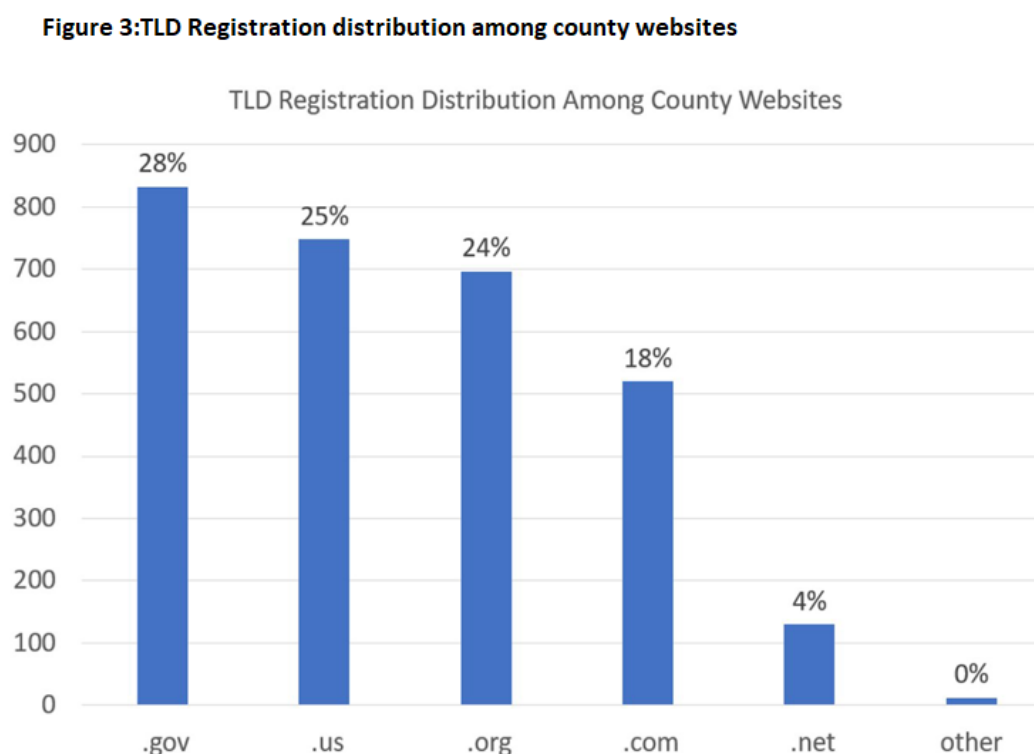
to note that 95% of state and county government sites that did not support HTTP still had port 80 open.

Figure 2: Websites checked for HTTP and HTTPS



The next “Best Practice” we examined was the TLD designation. Determining the TLD domain registration is an easy process as the domain suffix is used to provide proper domain

name resolution. While our custom CPP program was loading each state and county domain for analysis, it also collected the domain suffix (.org, .gov, etc.) into Figure 3.



Based on the study of the 2939 state and local government websites examined, only 28% (827) websites use a .gov domain and 25% (749) used a .us domain. A .us domain requires the registrant to be a US citizen, US organization or a have a presence in the US. There is no Federal vetting to the .US registration process, therefore anyone can register any domain as a .us (or any other domain suffix for that matter). Since it is not mandatory for a state or local government website to hold a .gov domain suffix, it becomes very difficult for a citizen to determine a legitimate government site for a fake one. As we have seen, threat actors are very skilled at mimicking actual sites, but with malicious content. Figure 4 represents the research of state and county domains broken down by population categories. 50% of the highest population counties used .gov domains and the lowest

Figure 4:TLD Domain Registration by population category

.com	17.69%	.gov	28.31%
1 to 75,000	80.77%	1 to 75,000	65.87%
75,001 to 149,999	7.12%	75,001 to 149,999	9.62%
150,000 to 249,999	5.38%	150,000 to 249,999	6.73%
250,000 to 499,999	2.88%	250,000 to 499,999	6.01%
500,000 to 999,999	2.31%	STATE	5.89%
1,000,000	0.96%	500,000 to 999,999	3.49%
STATE	0.58%	1,000,000	2.40%
.net	4.42%	.org	23.72%
1 to 75,000	76.15%	1 to 75,000	73.46%
75,001 to 149,999	10.77%	75,001 to 149,999	11.62%
150,000 to 249,999	4.62%	150,000 to 249,999	4.73%
250,000 to 499,999	3.85%	500,000 to 999,999	4.59%
500,000 to 999,999	3.08%	250,000 to 499,999	4.30%
1,000,000	1.54%	1,000,000	1.29%

.us	25.45%
1 to 75,000	77.27%
75,001 to 149,999	11.50%
150,000 to 249,999	5.61%
250,000 to 499,999	3.74%
500,000 to 999,999	1.47%
1,000,000	0.40%

other	0.41%
1 to 75,000	91.67%
250,000 to 499,999	8.33%

populated counties use a .gov with only a 28% adoption. Because the cost of a .gov registration is so much higher than any other TLD registration, it is possible that funding may be a concern. In addition, it is possible that there is a lack of understanding on the criteria citizens use to view a site as a legitimate government site. The wide spectrum of county government TLD usage in Figure 3 indicates that federal standardization, assistance and mandates are needed to require a .gov TLD registration for government sites. Also, we recommend that the Federal government should eliminate the financial impact for government agencies to use a .gov TLD.

Next, we examine the use of CA's as a Best Practice. By utilizing CA's within the same country, Governments can reduce root of trust and increase legal accountability. A root certificates country is determined by the country field in its certificate information. The findings of this study reveal that, 29% of all certificates were issued by 'Let's Encrypt' with Sectigo occupying second place with 18%. Only 1% of certificates were self-signed. Table 2 shows the distribution of Country codes between 2462 (not all counties returned certificate information) state and county websites examined, with 97% of sites having C.A.'s that originated from the U.S.

Table 2:Certificate Country Code

Certificate Country Code	Percent of Total Counties examined
US	81.83%
Unknown	16.16%
BE	1.33%
GB	0.48%
CH	0.14%
RU	0.07%
Grand Total	100.00%

As we have seen in the past research, utilizing a non-US C.A. can create security issues, such as a public key compromise and information leak, in addition to legal complexities if a breach occurs. While most sites used US based C.A.'s, there is a higher level of compromise risk with the 4% that utilize non-U.S. C. A's. We recommend that sites that utilize C.A's from other countries change to a US based on at their earliest convenience.

Ports are numbers that are used in TCP and UDP protocols for identification of services listening for communications on a workstation or server. Well known applications like port 80 for HTTP, or port 443 for HTTPS are often available in web servers as those applications are listening for web traffic requests. Risk increases when web servers utilize applications that are often

exploited due to misconfiguration, unpatched vulnerability or poor/non-existent security rules. Table 3 shows the breakdown of services open on the 2939 examined state and county websites. This implies that a website is not properly maintained as many of these services have more secure options available. A port is not open if there is no application listening on it. This means that any internet communications directed at this port number will get processed by the server. Open ports expose the listening services to exploit, which increases a server's likely hood for exploit.

Table 3:Open risky ports by population category

Population Category	Percent of Total Sites Examined
1 to 75,000	73.77%
75,001 to 149,999	10.14%
150,000 to 249,999	5.61%
250,000 to 499,999	4.39%
500,000 to 999,999	2.99%
STATE	1.77%
1,000,000	1.33%
Grand Total	100.00%

Based on the survey performed as shown in Table 3, 40% (1191) web servers had ports open other than 80 and 443, the traditional web traffic ports. The state of Illinois website has 991 open ports followed by the Bledsoe County, TN website with 647 open ports and Union County,

SC website with 599 open ports. Table 4 shows the number of servers with open ports based on protocol.

Table 4: Risky open services

Protocol	Number of Websites with Risky Services
RDP	40
SSH	591
DNS	396
SMTP	79
SMB	16
SQL	19
telnet	61
netbios	1
FTP	684

File Transport Protocol (FTP) is an outdated and insecure protocol and uses port 21. FTP does not utilize any encryption for both data transfer and authentication and there are more secure options available for web administrators, such as Secure FTP (SFTP). Therefore, it is not recommended that the service is used, and the port should be disabled. Based on the research, over 23% (684) of the state and county government sites examined had port 21 enabled. The use of FTP on the 684 servers that use FTP implies a lack of proper site administration, lack of security prioritization and a lack of understanding. Implementing SFTP is a more secure option to transfer files to\from a server other than FTP.

Secure Shell (SSH) is used for remote management and utilizes port 22. While it is generally considered secure, it requires proper key management and configuration to reduce its risk of exploit. It is not recommended that port 22 is accessible via the internet unless it is properly

secured. It is perfectly acceptable to use the SSH for remote management of a webserver but it requires much more configuration to be secure. There are better options available such as utilizing a virtual private network (VPN) to securely connect to the server to perform administration tasks. Based on the research, over 20% (591) of the state and county government websites examined had port 22 enabled.

Telnet, the predecessor to SSH, utilizes port 23. It is no longer considered secure and is frequently abused by malware. Based on the research, over 2% (61) of the state and county government websites examined had port 23 enabled. Utilizing this service on an internet facing webserver would imply lack of server administration knowledge or perhaps malicious activity. We advise to discontinue telnet, even for internal network connections. We recommend implementing SFTP with a VPN for site administration tasks. Telnet data is sent in clear text which means it can be easily read by looking at the web communications packet details.

Simple Mail Transport Protocol (SMTP) utilizes port 25 and is used to send, receive and/or relay outgoing mail between e-mail senders and receivers. If not properly secured, it can be abused for spam e-mail distribution, remote code execution or authentication failures. Attackers can use servers that host SMTP services as a launch pad for a larger malicious campaign. It is not recommended that state and county web servers should also be used as an e-mail distribution system. Therefore, the port should be disabled. Based on the research, over 3% (79) of the state and county websites examined had port 25 enabled. Utilizing this service on an interfacing webserver would imply lack of server administration and knowledge.

Domain Name Service (DNS) is often used for DDoS attacks and utilizes port 53. DNS is necessary for the proper routing of internet traffic. It is not advisable to have DNS and webservices hosted on the same state and county webserver, as it minimizes error handling if the server is down

or under attack. Therefore, in the spirit of proper server administration, port 53 should be disabled and the DNS services moved to a server better suited for DNS duty. Based on the research, over 14% (396) of the state and county websites examined had port 53 enabled.

NetBIOS, a legacy protocol that uses port 139, is primarily used for file and printer sharing. A state and local county government website should not be using NetBIOS for a sharing service; therefore, the port should be disabled. Based on the research, only <1% (1) of the state and county websites examined had port 139 enabled.

Server Message Blocks (SMB) uses port 445 for its sharing capabilities of files and printers. SMB was exploited in 2017 by the famous WannaCry attack. Therefore, port 445 should be disabled, and a state and local counties internet-facing web server should not be used for file and print services. Based on the research, <1% (16) of the state and county government websites examined had port 445 enabled. The port active on a webserver would imply improper server maintenance and understanding.

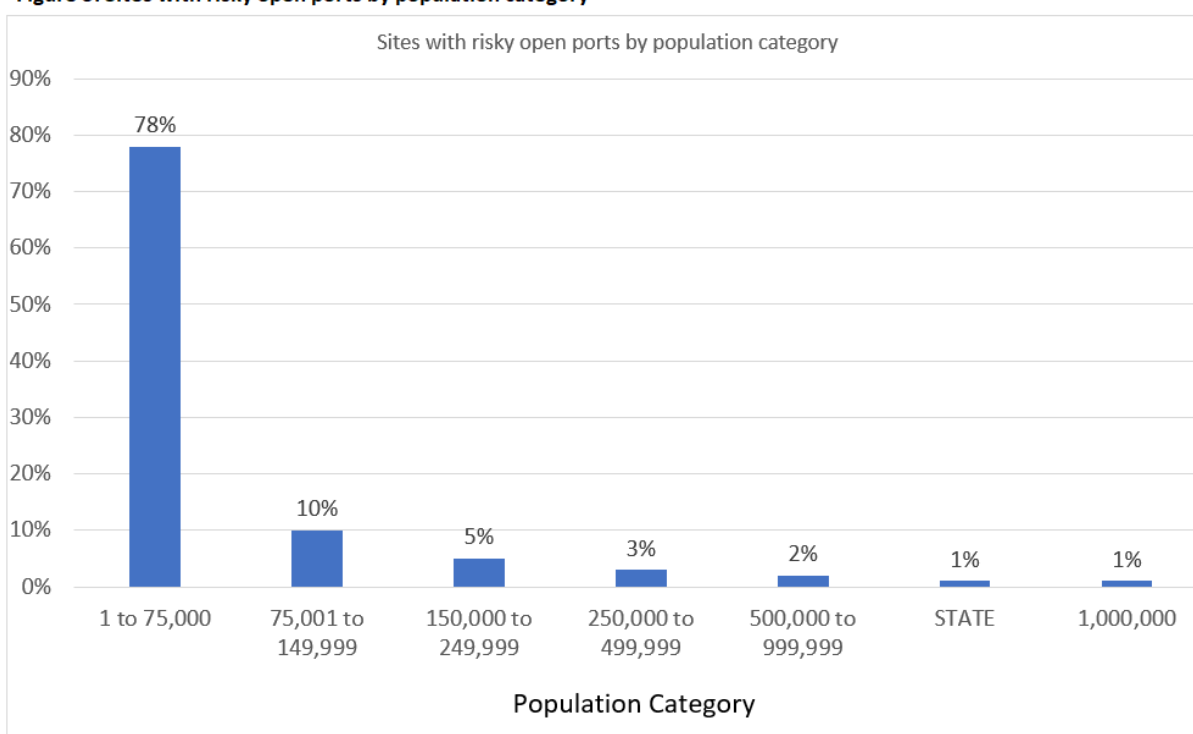
The default ports for Structured Query Language (SQL) are ports 1433, 1434, and 3306. These ports are easily able to be used for malware distribution and enabling them on an internet facing interface will allow external parties to directly hit privileged data stores without any intelligent monitoring or filtering. Typically, these ports are for internal use only and exposure to internet traffic is usually a misconfiguration, malicious actor or lack of understanding by administrators (Serious-Security-Dont-Let-Your-Sql-Server-Attack-You-with-Ransomware, 2019). Based on the research, <1% (19) of the state and county government websites examined had the default SQL enabled.

Remote Desktop (RDP) uses port 3389 and is arguably one of the riskiest ports to have open on an internet-facing server. RDP is utilized to exploit various vulnerabilities in remote

desktop protocols, as well as weak user authentication. There have been many compromises because of the RDP service being accessible from the internet to a server (Top-Exploits-Used-by-Ransomware-Gangs-Are-Vpn-Bugs-but-Rdp-Still-Reigns-Supreme, 2021). Remote desktop vulnerabilities are commonly used in real-world attacks, with the last example being the BlueKeep vulnerability. Based on the research, 1% (40) of the state and county government websites examined had port 3389 enabled. There is no necessity to have enable Remote Desktop on an internet accessible interface, thus enabling untrusted users to attempt connection to the webserver. Typically enabling RDP protocol on an internet facing interface is usually the result of lack of understanding by administrators, a malicious actor, or misconfiguration.

Based on the information presented in Figure 5, counties within the population category ‘1 to 75,000’ contain the highest number of open ports (listening services) per server. We believe this would imply that some counties have not prioritized web security.

Figure 5: Sites with risky open ports by population category

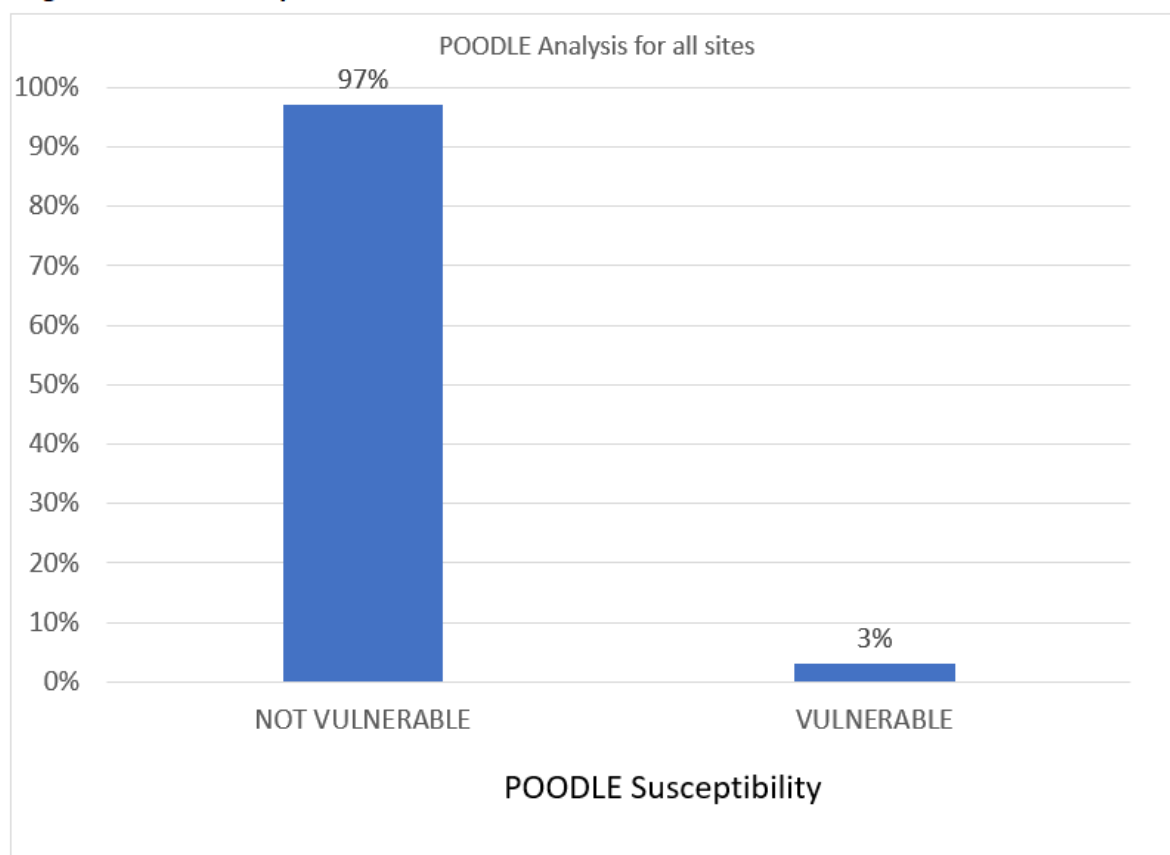


5.2 LEGACY EXPLOIT FINDINGS

In this section, we will discuss the results of our legacy exploit checks. The legacy exploits examined by this research are POODLE, HeartBleed, FREAK, DROWN and SWEET32. These legacy exploits were selected because they are very effective and their implementation is very well documented, making them easy to invoke by almost anyone. These legacy exploits are simple and inexpensive to mitigate, therefore being vulnerable to these exploits would indicate improper or poor site administration.

5.2.1 POODLE FINDINGS

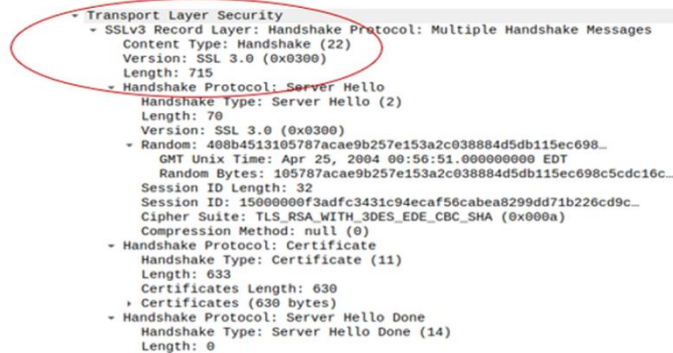
Figure 6: POODLE Analysis for all sites



As discussed in previous Chapters, a POODLE attack is an attack against the TLS stack which an attacker can force a client to use weaker SSL encryption. Figure 6 shows the number of county

sites susceptible to a POODLE attack. Of the state and local county government sites examined that accepted TLS connections, 92 sites (3% of the study sample) were susceptible to a POODLE attack. Example 3 shows an analysis of a packet using a packet analyzer. By looking at the packet details, we can see that our sampled server accepted communications using SSL not TLS. This means that it possible for a malicious attacker to request weaker SSL communications instead of using TLS. Only 1 site in the ‘+1,000,000 population” category had susceptibility to a POODLE attack, while other categories had multiple sites that were susceptible. As we can see in Example 3, a successful response for a state and local county webserver is accepted utilizing SSL 3.0, making it susceptible to a POODLE attack.

Example 3 - POODLE packet analysis



```

- Transport Layer Security
  - SSLv3 Record Layer: Handshake Protocol: Multiple Handshake Messages
    Content Type: Handshake (22)
    Version: SSL 3.0 (0x0300)
    Length: 715
  - Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: SSL 3.0 (0x0300)
  - Random: 408b4513105787acae9b257e153a2c038884d5db115ec698...
    GMT Unix Time: Apr 25, 2004 00:56:51.000000000 EDT
    Random Bytes: 105787acae9b257e153a2c038884d5db115ec698c5cdc16c...
    Session ID Length: 32
    Session ID: 1500000f3adfc3431c94ecaf56cabea8299dd71b226cd9c...
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
    Compression Method: null (0)
  - Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 633
    Certificates Length: 630
    Certificates (630 bytes)
  - Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0
  
```

5.2.2 DROWN FINDINGS

Next we examined the DROWN legacy exploit. Example 4 shows an analysis of a Drown susceptible packet using the Wireshark packet analyzer. An examination of the ServerHello message reveals a successful connection with SSL 2.0. As indicated by authors Aviram et al., in the research “DROWN: breaking TLS using SSLv2”, any server that accepts a connection on SSL 2.0 is susceptible to the DROWN attack (Aviram et al., 2016). In addition, the authors point out

that any additional sever that utilizes the same certificate as a server that uses SSL 2.0, regardless of the TLS version, can be compromised (Aviram et al., 2016).

Example 4 – DROWN packet analysis

```

- Transport Layer Security
  - SSLv2 Record Layer: Server Hello
    [Version: SSL 2.0 (0x0002)]
    Length: 672
    Handshake Message Type: Server Hello (4)
    Session ID Hit: False
    Certificate Type: X.509 Certificate (1)
    Version: SSL 2.0 (0x0002)
    Certificate Length: 627
    Cipher Spec Length: 18
    Connection ID Length: 16
  - Certificate: 3082026f308202190210622521a645a82766a70e2f
    - signedCertificate
      - serialNumber: 0x622521a645a82766a70e2a1c9bf5d5f6
      - signature (md5WithRSAEncryption)
      - issuer: rdnSequence (0)
      - validity
      - subject: rdnSequence (0)
      - subjectPublicKeyInfo
      - algorithmIdentifier (md5WithRSAEncryption)
      - Padding: 0

```

Of the 2939 state and local county government websites examined by this research, only 7 (.096%) were susceptible to a DROWN attack. 6 of the 7 sites that were susceptible to a DROWN attack were in the two lowest population categories. DROWN can be mitigated by either disabling SSLv2, patching OpenSSL or updating the server OS.

5.2.3 FREAK FINDINGS

Next, we examined the FREAK legacy vulnerability. Of the 2939 state and local county government websites examined, only 9 (.19%) were susceptible to a FREAK attack. Example 5, shows the packet details that can be exploited by the FREAK attack. The details reveal a state and county server connection acceptance using an exportable cipher. As we can see in the packet analysis, a weaker export cipher was selected to secure communications. A change in the registry

Example 5 – FREAK packet analysis

```

- Transport Layer Security
  - TLSv1 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 74
  - Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: TLS 1.0 (0x0301)
  - Random: 604553302ad6c6a1a27234aaacd65a688cc2f46aa627abfc...
    GMT Unix Time: Mar 7, 2021 17:26:56.000000000 EST
    Random Bytes: 2ad6c6a1a27234aaacd65a688cc2f46aa627abfc5e58793f...
    Session ID Length: 32
    Session ID: a666d14dda7e8bf008205fa5b974429078578db3b6e0c7e4...
    Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
    Compression Method: null (0)

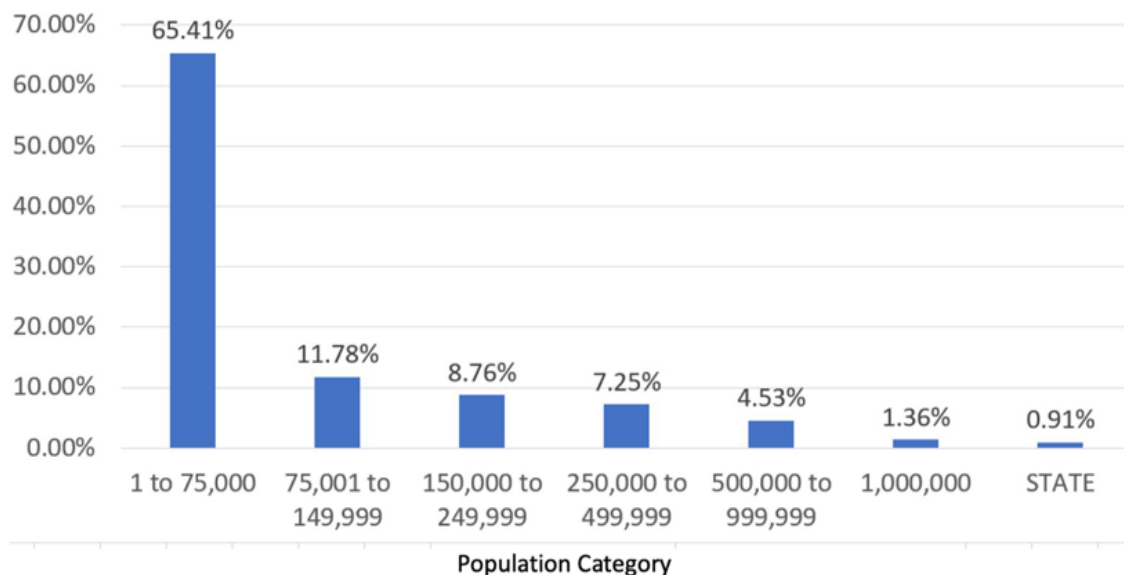
```

can be made to disable the use of export ciphers or patch OpenSSL will prevent the exploit of this vulnerability. Proper site patching and maintenance can mitigate this attack.

5.2.4 SWEET32 FINDINGS

Published over 4 years ago, SWEET32 remains a significant threat to our nations state and county government websites. Figure 7 shows that of the state and county websites examined on 662 (23%) were using legacy block ciphers and they are susceptible to the Sweet32 attack. 432 of the sites that were susceptible to the SWEET32 attack were in the lowest population category.

Figure 7: Percent of SWEET32 at risk sites by population category



An examination of the packet details in Example 6 shows that the sample server allowed a secure connection using a 3DES cipher suite. This could allow a man-in-the-middle attacker to recover small portions of the secure data as plaintext by exploiting a flaw in the 3DES cipher.

Simply, applying openssl security update RHSA-2016:1940 will mitigate this threat. The fact that 662 state and county websites are still vulnerable to this exploit point to a lack of system

Example 6 – SWEET32 packet analysis

```

- Transport Layer Security
- TLSv1 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 80
- Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 76
  Version: TLS 1.0 (0x0301)
- Random: 604556bcc5fb603912c44bae2f8f3244fdb68c7332b6b79d...
  GMT Unix Time: Mar  7, 2021 17:42:04.000000000 EST
  Random Bytes: c5fb603912c44bae2f8f3244fdb68c7332b6b79d444f574e...
  Session ID Length: 32
  Session ID: 4cb877172e33f0bb75e064f25be4ff35b2ac6d87aca0e408...
  Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
  Compression Method: null (0)
  Extensions Length: 4
- Extension: server_name (len=0)
  Type: server_name (0)
  Length: 0

```

administration best practices.

5.2.5 HEARTBLEED FINDINGS

Based on this study, it was discovered that no state or county government website was susceptible to a HeartBleed attack. This would imply that the remediation of this vulnerability has been easy to implement, and/or highly publicized to where business leaders put emphasis on the update. Table 5 shows the number of sites still susceptible to these legacy exploits. SWEET32 is the least mitigated exploit. Disabling weak block ciphers for the particular running web hosting operating system will easily resolve this vulnerability with little if any expense to the organization. Table 6 shows the county sites that were susceptible to all the surveyed legacy exploits but Heartbleed. These county sites are extremely vulnerable to exploit, if they have not already been compromised. This implies that there is a lack of proper site administration.

Table 5: Percent of vulnerable to legacy exploits

Legacy Exploit	Percentage of Susceptible Sites
FREAK	0.31%
SWEET32	22.52%
DROWN	0.24%
POODLE	3.13%
HeartBleed	0.00%

Table 6: Sites vulnerable to every checked exploit (except Heartbleed)

COUNTY SITE	SWEET32	FREAK	DROWN	POODLE
foardcountytexas.us				
childresscountytexas.us				
kentcountytexas.us				
motleycountytexas.us				
kingandqueenco.net				
clallam.net				
kingcountytexas.us				



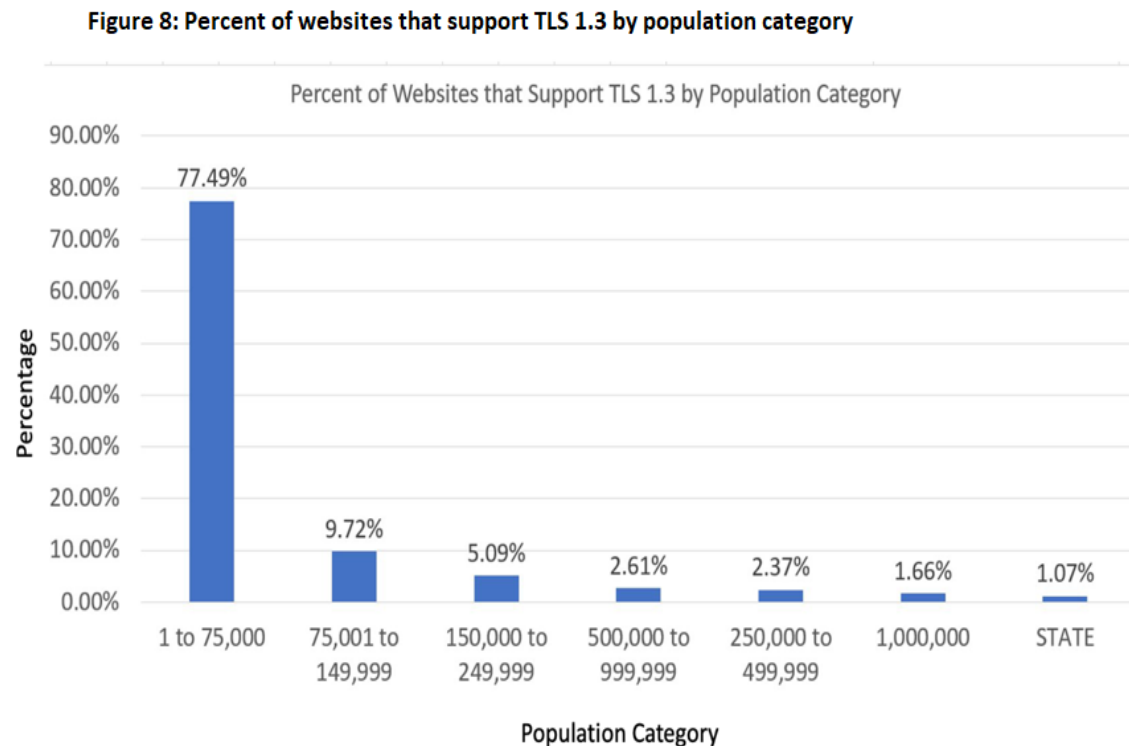
= VULNERABLE

5.3 EMERGING TECHNOLOGY ADOPTION

In this section, we examine the adoption of new and emerging technologies within website communications. We checked for adoption of HTTP/2, HSTS, and TLS version 1.3. These items were selected because they are easy and inexpensive to implement. By not implementing these new security features could imply a lack of security focus or lack of resources needed to implement new technology features

5.3.1 TLS 1.3 ADOPTION

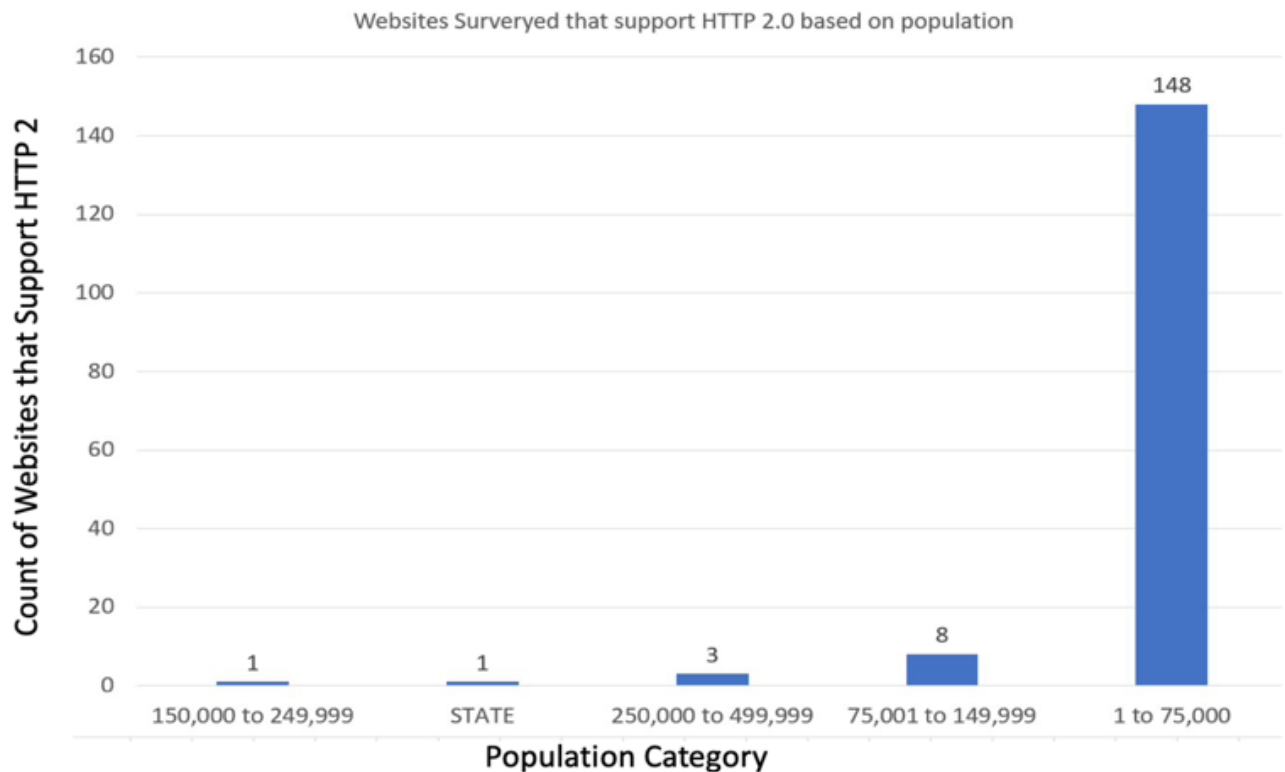
As we have seen in our past research, TLS 1.3 improves security by removing old, weaker cipher suites. Our research shows that 29% of all state and county government websites examined accepted TLS 1.3 connections. Also, 55% of the county sites support TLS 1.2. Figure 8 shows the distribution of sites vs TLS level to population category.



5.3.2 HTTP/2 ADOPTION

HTTP/2 provides greater security over standard HTTP 1.1 because HTTP/2 requires TLS encryption to be used as indicated by the past research. Our research conducted shows that out of 2939 sites examined, only 5% (156) accepted connection from HTTP/2, (Figure 9) with the ‘less

Figure 9: Websites that support HTTP/2 by population category



than 150,000’ population category having the largest acceptance. This could imply that counties that are in the ‘150,000 to 249,999’ may be more focused on innovation than counties in other population groups.

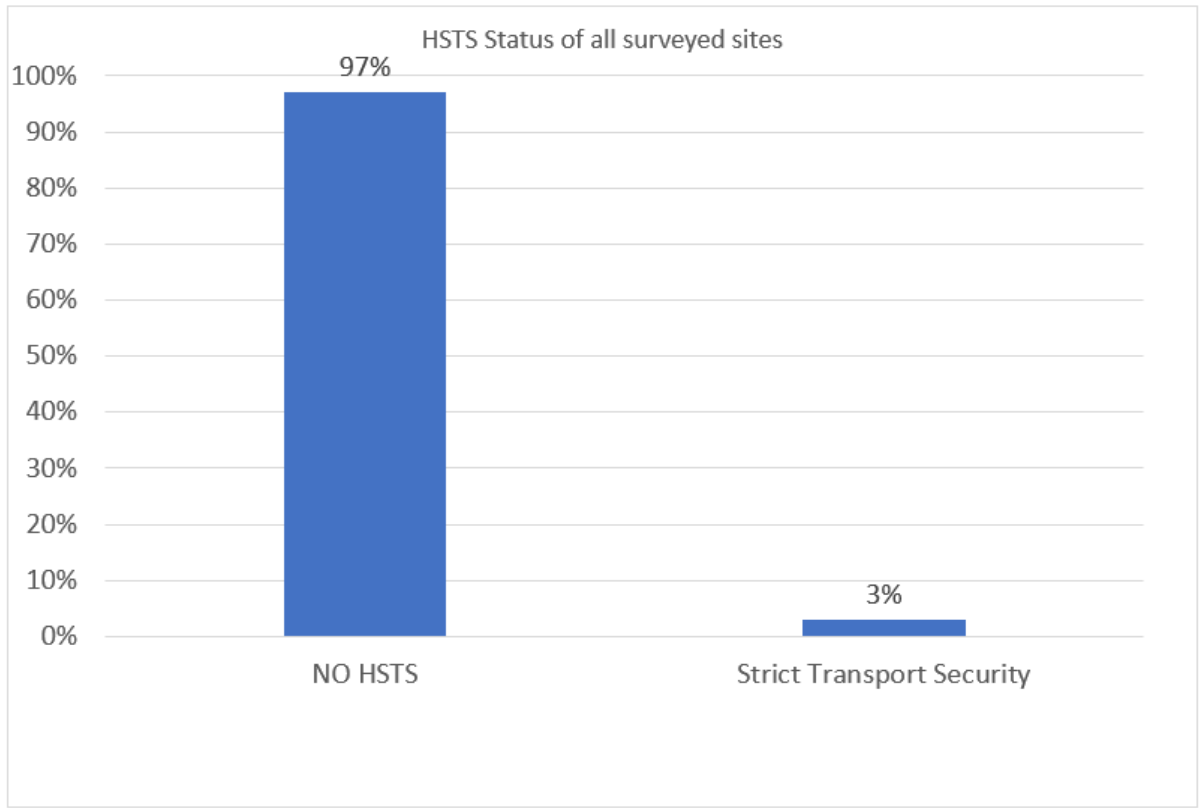
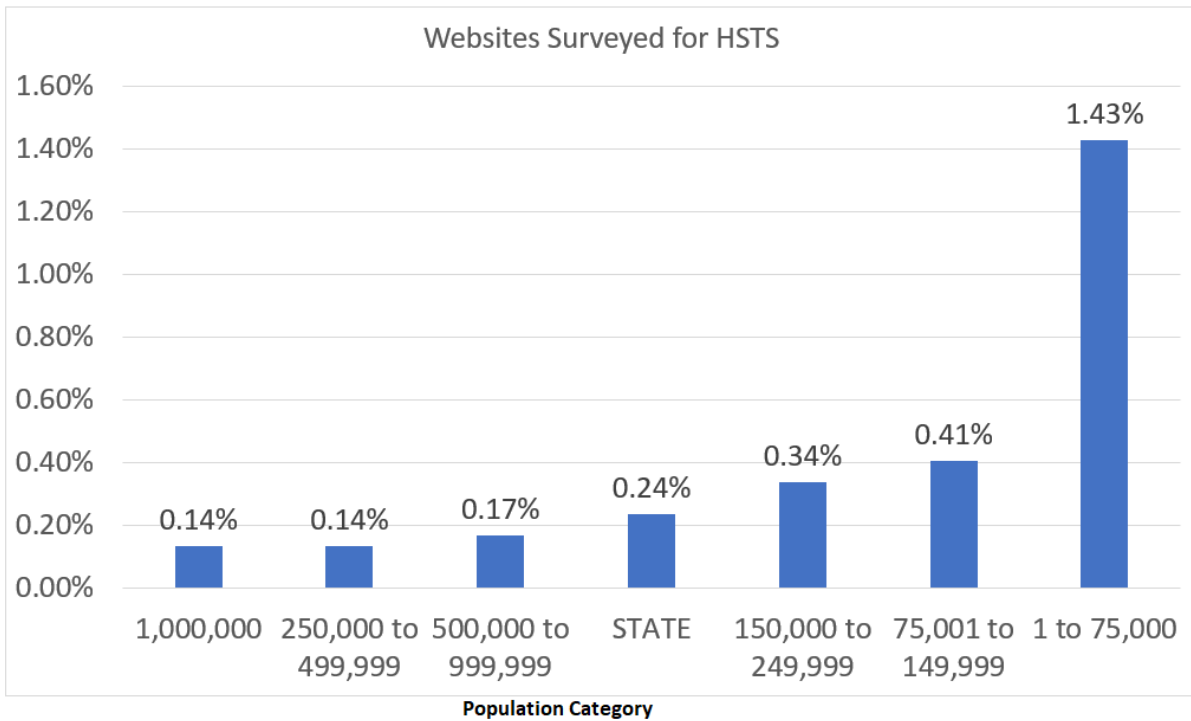
5.3.3 HSTS ADOPTION

HTTP Strict Transport Security (HSTS) is a new web policy that prevents browsers from being able to select a weaker or downgraded level of TLS. This improves security by ensuring that only the strongest TLS encryption is used. Figure 10 shows that based on the research performed

against 2939 state and county government websites, only 3% (68) supported HSTS. The highest percentage of adoption of HSTS was by state and county governments in the 1,000,000+ population category, with a 3% adoption percent. The research conducted shows that out of 2939 sites examined, only 3% (99) accepted a connection from HTTP/2. The highest percentage of adoption of HSTS was by state and county governments in the ‘1,000,000+’ population category. The category had a 3% adoption percent. The research conducted shows that out of 2939 sites examined, only 3% (99) accepted a connection from HTTP/2 (Table 7) with the ‘less than 75,000’ population category having the largest acceptance of 7%. An interesting note is that no site examined support HTTP/2 and HSTS. Figure 11 shows that the ‘1 to 75,000’ population has the highest adoption rate of HSTS/ This could imply that counties that have the least populations may be more innovative than those in other categories. In the next section we will present the final analysis of our results.

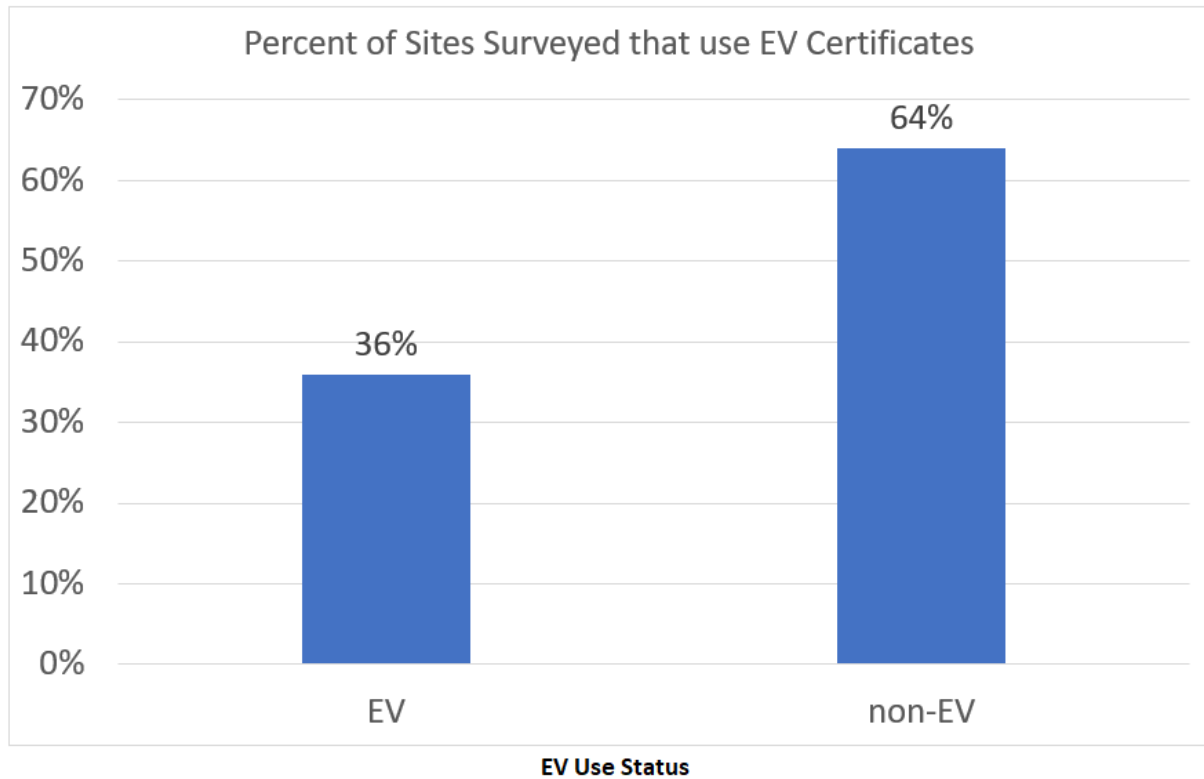
Table 7: HSTS and HTTP/2 Adoption

New Technology	Adopted Sites	Not Adopted	Percent of examined sites
HSTS	68	2007	3%
HTTP 2	99	1976	3%

Figure10: HSTS status of all survey sites**Figure 11: HSTS status of all survey sites by population category**

As we have seen in the past research Extended Validation certificates require a more rigorous vetting process before being assigned by the certificate authority. Based on the results 36% of sites examined use EV certificates (Figure 12).

Figure 12: Percentage of sites that support EV Certificates



5.4 ANALYSIS

In this section, we will complete our analysis by comparing the results of states and regions of the country. In addition, we will look at the best and worst counties and how they compare to each other. By comparing the states together, we can get a better understanding of how each state is susceptible.

If we examine each region of the U.S., the data reveals that the average county website benchmark of each region is 12 with the exception of the Southwest region which is 10, largely due to Texas (Table 8).

Table 8: average website benchmark by region

Region	Average Site Benchmark
SouthWest	10
Midwest	12
Northeast	12
Southeast	12
West	12

Figure 13 shows the average benchmark of all state and county government websites sorted by state. Rhode Island is the state with the most secure county websites, followed closely by Kentucky. Texas is the state with the least secure county websites. Figure 13 shows the state and county government sites that have the highest benchmark. It should be noted that no site received a perfect benchmark.

Figure 14 shows the state and county government sites that have the highest benchmark. It should be noted that no site received a perfect benchmark.

Figure 13: Average benchmark of county websites by state

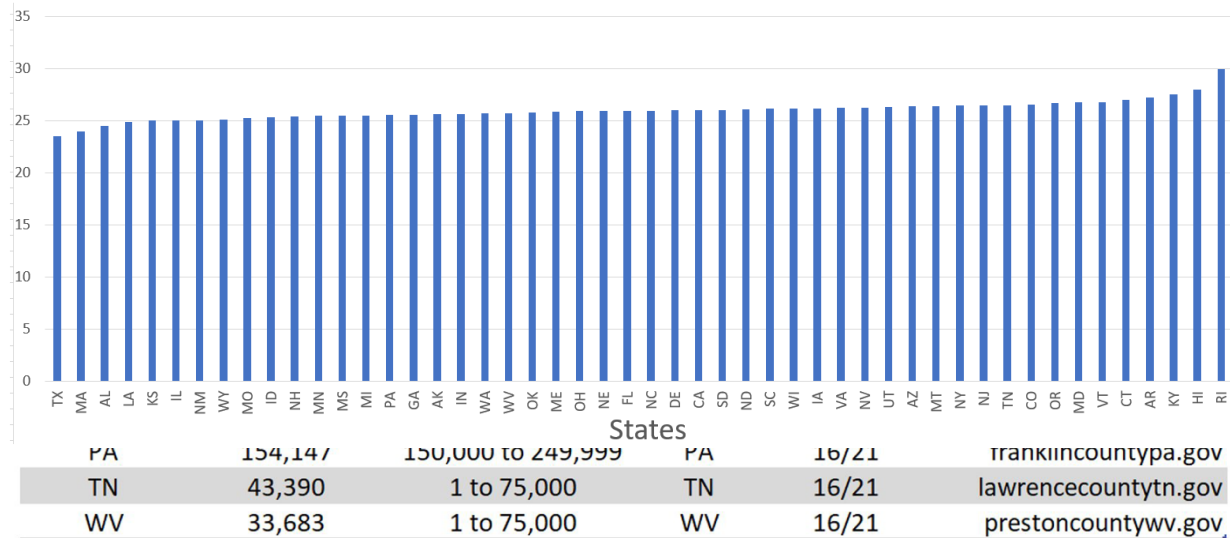


Figure 15 shows the state and county government websites with the lowest benchmarks. As we can see from the survey, Texas is the state with the lowest benchmark, occupying 6 of the bottom 9 places. It is not surprising that Texas has had some significant cyber events perpetrated against many of its local governments (Texas-Towns-Hit-with-Ransomware-Attack-in-New-Front-of-Cyberassault, 2019) .

Figure 15 – County Sites with a < 5 Score

State	population	population category	State2	score final	Website
NC	54,925	1 to 75,000	NC	5/21	wataugacounty.org
TX	7,304	1 to 75,000	TX	4/21	dallam.org
TX	1,275	1 to 75,000	TX	5/21	foardcountytexas.us
TX	7,253	1 to 75,000	TX	5/21	childresscountytexas.us
TX	647	1 to 75,000	TX	5/21	kentcountytexas.us
TX	237	1 to 75,000	TX	5/21	kingcountytexas.us
TX	1,252	1 to 75,000	TX	5/21	motleycountytexas.us
VA	7,042	1 to 75,000	VA	4/21	kingandqueenco.net
WA	75,392	75,001 to 149,999	WA	4/21	clallam.net

In summary, the research shows that any state, local government, tribal or territorial website can be secured regardless of population size. Generally, the larger the population, the larger the budget for Information Technology needs. Information Technology funding makes up of roughly 5% to 10% of a counties overall operating budget according to Shannon Tufts of the UNC school of Government (S. Tufts, personal communication, Dec, 2020). Our study shows that counties with the lowest populations have some of the most secure and some of the most insecure county websites. Clark County Iowa, has a 9360 population, yet it is one of the most secure county websites. While Clallam county, Washington has a population of 75,392 and is the least secure. This would indicate that many of these insecurities can be remediated with little funding or no funding necessary. County population size does not seem to be a deciding factor to county website security. We believe that this point system should be implemented by IT professionals to benchmark their local government sites. In addition, browser companies like Google Chrome should scrutinize the security of government sites more carefully. There is an opportunity for private consultants to help local governments solve this problem. Federal funding and mandates may also be needed.

Based on the research, HTTPS adoption is at 84%, yet most county websites have port 80 open, increasing a site's attack surface, which makes it more susceptible to malicious manipulation. In addition, many county websites have risky ports open, which further increases a site's risk of compromise. Remote Desktop Protocol (RDP), arguably the riskiest port to have open on an internet-facing interface, is available and listening on 41 county websites. Top-level .gov domain registration is at 28%, followed by .us and .org. 96% of all websites examined had certificates issued from the US, yet the adoption of Extended Validation certificates are only used by 36% of the counties examined. Texas is the state with the least secure county websites

on average. At the same time, Rhode Island has the highest average security benchmark, followed closely by Kentucky, yet no county received a perfect benchmark. The study will conclude in the next section with a final summary and a need for further research.

CHAPTER 6. CONCLUSION

To conclude, the background has shown that the United States considers state and county government web systems as critical infrastructure and is a significant target by malicious threat actors. This study has shown that our nation's state and county government websites are not as secure and maintained as they should be. This study indicates the need for more federal mandates and grant assistance for counties in the <150,000 categories. The methodology used to prove this study is gathered with Nmap, Curl, OpenSSL, and personal query.

6.1 SUMMARY

State and county websites do not widely adopt new emerging technologies such as TLS 1.3, HSTS, and HTTP/2. Extended Validation certificates have the most adoption by counties, with 36% of the sites using them. The proper .gov domain registration, one of the critical components of instilling citizen confidence, is only used by 28% of the state and county websites examined. While 97% of state and county sites had certificates signed by U.S. organizations, 3% were from outside the U.S. I.T. house-keeping items such as the use of self-signed or expired certificates seemed to have been resolved and afflict only >1% of the sites examined, but 64% of state and county government websites had additional risky server ports open and exposed to the internet. In addition, 40 state and county websites had remote desktop protocol (RDP) port open

to the internet. Site administration is a problem as evident by the number of web servers with open risky ports.

Based on the research performed, the legacy exploits have largely been mitigated. Legacy Exploits such as POODLE, Heartbleed, DROWN, and FREAK show very little risk to our national infrastructure with the exception of SWEET32. Over 600 county websites sites are still susceptible to the SWEET32 attack. The SWEET32 attack still poses a significant risk to over 25% of our nation's citizen serving, county informational websites.

The literature review that we have presented has shown that proper patching and site administration can mitigate malicious attacks against the TLS\SSL stack. Also, it shows the importance of E.V. certificates, HSTS, TLS 1.3, C.A. (Certificate Authority) country origin, HTTP/2 adoption, and domain registration can further protect a site from malicious manipulation. Many of these mitigations are free to implement such as disabling old cipher suites and unnecessary services, patching openssl and operating systems, and enforcing TLS levels.

Local governments are the fabric that connect the nation, the states and its citizens to services. Because public-facing local government websites are the front-line for delivering official information (such as vaccine information) and accessing local government services, attacks targeting these websites can cause widespread panic and citizen instability. Also, malicious actors can use a poorly secured government site to steal citizen credentials, expose sensitive citizen data, and act as a pivot point for further malicious activity. This research is vital in our understanding of our susceptibility to cyber-attacks against our state and local governments. This research shows that state and county government websites are not as secure as they should be and that citizen confidence, data, and stability are at risk. We believe that this point system should be implemented

by IT professionals to benchmark their local government sites. In addition, browser companies like Google Chrome should scrutinize the security of government sites more carefully, and alerting users to the trustworthiness of the site based on our scoring. There is an opportunity for private consultants to help local governments solve the problem of low benchmark trustworthiness scoring. Federal funding and mandates may also be needed.

6.2 FURTHER RESEARCH

Further research is needed to examine additional state and county citizen-centric websites, such as the local law enforcement, local hospital, tribal and legal websites. Additionally, a future direction is to track the remediation rates for the state and county web systems over time. This study will aid our holistic understanding of the nation's cyber-attack susceptibility and provide evidence for a need for federal mandates for cybersecurity guidelines aimed at all types of citizen-facing government websites.

CHAPTER 7. REFERENCES

- 1) Vijayan, J. (2018, October 25). *County election websites can be easily spoofed to spread misinformation*. Dark Reading.
<https://www.darkreading.com/vulnerabilities-threats/county-election-websites-can-be-easily-spoofed-to-spread-misinformation/d/d-id/1333132>
- 2) Hsiao, H.-C., Kim, T. H.-J., Ku, Y.-M., Chang, C.-M., Chen, H.-F., Chen, Y.-J., Wang, C.-W., & Jeng, J. (2019, May). *An investigation of cyber autonomy on government websites*. In The World Wide Web Conference (WWW '19). Association for Computing Machinery, New York, NY, USA, 2814–2821. <https://doi.org/10.1145/3308558.3313645>
- 3) Dwoskin, E., & Timberg, C. (2018, August 21). *Microsoft says it has found a Russian operation targeting U.S. political institutions*. Washington Post.
https://www.washingtonpost.com/business/economy/microsoft-says-it-has-found-a-russian-operation-targeting-us-political-institutions/2018/08/20/52273e14-a4d2-11e8-97ce-cc9042272f07_story.html?noredirect=on&utm_term=.db741731087b
- 4) Mavrogiannopoulos, N., Vercauteren, F., Velichkov, V., & Preneel, B. (2012, October). *A cross-protocol attack on the TLS protocol*. In Proceedings of the 2012 ACM (Association for Computing Machinery) conference on Computer and communications security (CCS '12). Association for Computing Machinery, New York, NY, USA, 62–72. <https://doi.org/10.1145/2382196.2382206>
- 5) Clark, J., & van Oorschot, P.C. (2013). *SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements*. 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 511-525, [doi: 10.1109/SP.2013.41](https://doi.org/10.1109/SP.2013.41).
- 6) Anja Feldmann, A., Cittadini, L., Mühlbauer, W., Bush, R., & Maennel, O. 2009. *HAIR: hierarchical architecture for internet routing*. In Proceedings of the 2009 workshop on Re-architecting the internet (ReArch '09). Association for Computing Machinery, New York, NY, USA, 43–48. DOI:<https://doi.org/10.1145/1658978.1658990>

- 7) Joshua Sunshine, Serge Egelman, Hazim Almuhiemedi, Neha Atri, and Lorrie Faith Cranor. 2009. *Crying wolf: an empirical study of SSL warning effectiveness*. In Proceedings of the 18th conference on USENIX security symposium (SSYM'09). USENIX Association, USA, 399–416.
- 8) zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman. 2013. *Analysis of the HTTPS certificate ecosystem*. In Proceedings of the 2013 conference on Internet measurement conference (IMC '13). Association for Computing Machinery, New York, NY, USA, 291–304. DOI:<https://doi.org/10.1145/2504730.2504755>
- 9) Möller, Bodo; Duong, Thai & Kotowicz, Krzysztof. *This POODLE Bites: Exploiting the SSL 3.0 Fallback*, report, September 2014; (<https://digital.library.unt.edu/ark:/67531/metadc949502/>: accessed November 12, 2020), University of North Texas Libraries, UNT Digital Library, <https://digital.library.unt.edu>; crediting UNT Libraries Government Documents Department.
- 10) Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. Alex Halderman. 2014. *The Matter of Heartbleed*. In Proceedings of the 2014 Conference on Internet Measurement Conference (IMC '14). Association for Computing Machinery, New York, NY, USA, 475–488. DOI:<https://doi.org/10.1145/2663716.2663755>
- 11) govinfo. (2021). Code of Federal Regulations Chapter 102, Sub-Chapter 173. <https://www.govinfo.gov/app/details/CFR-2010-title41-vol3/CFR-2010-title41-vol3-part102-id2024>
- 12) Adrienne Porter Felt, Richard Barnes, April King, Chris Palmer, Chris Bentzel, and Parisa Tabriz. 2017. *Measuring HTTPS adoption on the web*. In Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17). USENIX Association, USA, 1323–1338.
- 13) govinfo. (2021). Code of Federal Regulations Chapter 102, Sub-Chapter 173. <https://www.govinfo.gov/app/details/CFR-2010-title41-vol3/CFR-2010-title41-vol3-part102-id2024>

- 14) Executive order -- improving critical infrastructure cybersecurity. (n.d.). Retrieved February 11, 2021, from <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
- 15) Pawel Szalachowski. 2019. EVLA: Extended-Validation Certificates with Location Assurance. In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '19). Association for Computing Machinery, New York, NY, USA, 73–79. DOI:<https://doi-org.mendel.csuniv.edu/10.1145/3327960.3332379>
- 16) Gareth Tyson, Shan Huang, Felix Cuadrado, Ignacio Castro, Vasile C. Perta, Arjuna Sathiaselalan, and Steve Uhlig. 2017. Exploring HTTP Header Manipulation In-The-Wild. In Proceedings of the 26th International Conference on World Wide Web (WWW '17). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 451–458. DOI:<https://doi-org.mendel.csuniv.edu/10.1145/3038912.3052571>
- 17) Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Jean Karim Zinzindohoue. 2017. A messy state of the union: taming the composite state machines of TLS. Commun. ACM 60, 2 (February 2017), 99–107. DOI:<https://doi-org.mendel.csuniv.edu/10.1145/3023357>
- 18) Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt. 2016. DROWN: breaking TLS using SSLv2. In Proceedings of the 25th USENIX Conference on Security Symposium (SEC'16). USENIX Association, USA, 689–706.
- 19) Ralph Holz, Jens Hiller, Johanna Amann, Abbas Razaghpanah, Thomas Jost, Narseo Vallina-Rodriguez, and Oliver Hohlfeld. 2020. Tracking the deployment of TLS 1.3 on the web: a story of

experimentation and centralization. *SIGCOMM Comput. Commun. Rev.* 50, 3 (July 2020), 3–15.

DOI:<https://doi-org.mendel.csuniv.edu/10.1145/3411740.3411742>

- 20) Konrad Wolsing, Jan R  th, Klaus Wehrle, and Oliver Hohlfeld. 2019. A performance perspective on web optimized protocol stacks: TCP+TLS+HTTP/2 vs. QUIC. In *Proceedings of the Applied Networking Research Workshop (ANRW '19)*. Association for Computing Machinery, New York, NY, USA, 1–7. DOI:<https://doi-org.mendel.csuniv.edu/10.1145/3340301.3341123>

- 21) Lohrmann, D. (2020). *State and Local Governments Face Iranian Hacking Threats*.

Govinfo. <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/state-and-local-governments-face-iranian-hacking-threats.html>

- 22) *Presidential Policy Directive -- Critical Infrastructure Security and*. (2013, May 23).

Whitehouse.Gov. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

- 23) *Information Technology Sector | CISA*. (2021). <https://www.cisa.gov/information-technology-sector>

Technology-Sector. <https://www.cisa.gov/information-technology-sector>

- 24) Prall, D. (2015, May 18). *Local government websites are first line of defense in emergencies*. American City and County.

<https://www.americancityandcounty.com/2015/05/18/local-government-websites-are-first-line-of-defense-in-emergencies/>

- 25) Mazarr, M. J. (2019, September 4). *“Hostile Social Manipulation” Is a Growing Threat to the United States*. “Hostile Social Manipulation” Is a Growing Threat to the United

States. https://www.rand.org/pubs/research_reports/RR2713.html

- 26) US Census Bureau. (2018, May 16). *Geographic Areas Reference Manual*. The United

States Census Bureau. <https://www.census.gov/programs-surveys/geography/guidance/geographic-areas-reference-manual.html>

- 27) *Information Technology Sector* / CISA. (2021). <https://www.cisa.gov/information-technology-sector>
- 28) Tufts, S. (2020, Dec 15). Personal Communication [Personal interview].
- 29) *top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme*. (2021). Zdnet.Com. <https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/>
- 30) *serious-security-dont-let-your-sql-server-attack-you-with-ransomware*. (2019). Nakedsecurity.Sophos.Com. <https://nakedsecurity.sophos.com/2019/05/25/serious-security-dont-let-your-sql-server-attack-you-with-ransomware/>
- 31) *texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault*. (2019). Www.Npr.Org. <https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault>
- 32) *state-local-government*. (2020). Whitehouse.Gov. <https://www.whitehouse.gov/about-the-white-house/our-government/state-local-government/>