Application Level Security: A Case Study of a Public Library

Abstract
Libraries have historically made great efforts to ensure the confidentiality of personally identifiable information (PII), but the rapid, widespread adoption of information technology and the Internet have given rise to new privacy and security challenges. Hypertext Transport Protocol Secure (HTTPS) is a form of Hypertext Transport Protocol (HTTP) that enables secure communication over the public Internet, and provides a deterministic way to guarantee data confidentiality so that attackers cannot eavesdrop on communications. HTTPS has been used for several years to protect sensitive information exchanges, but recent security exploits such as Firesheep have exposed the need to implement HTTPS in a more rigorous and pervasive manner. This report is intended to shed light on the state of HTTPS implementation in libraries, and to suggest ways in which libraries can evaluate and improve application security so that they can better protect the confidentiality of PII about library patrons.

Keywords: Application level security, personally identifiable information, information security, library

1. Introduction

Patron privacy is fundamental to the practice of librarianship in the United States. Libraries have historically made great efforts to ensure the confidentiality of personally identifiable information (PII), but the rapid, widespread adoption of information technology and the Internet have given rise to new privacy and security challenges. The USA PATRIOT Act, along with electronic surveillance efforts by the National Security Agency (NSA) and other government agencies, has further intensified privacy concerns about sensitive information that is transmitted over the public Internet when patrons interact with electronic library resources through online systems such as online public access catalog (OPAC).

Hypertext Transport Protocol Secure (HTTPS) is a form of Hypertext Transport Protocol (HTTP) that enables secure communication over the public Internet, and provides a deterministic way to guarantee data confidentiality so that attackers cannot eavesdrop on communications. HTTPS has been used for several years to protect sensitive information exchanges (e-commerce transactions, user authentication, etc.). In practice, however, security exploits such as Firesheep have demonstrated the relative ease with which an attacker can transparently eavesdrop on or hijack HTTP traffic by targeting gaps in HTTPS implementation. There is little or no evidence in the literature that libraries are aware of the associated vulnerabilities, threats, or risks, or that researchers have evaluated the use of HTTPS in library Web applications. This report is intended to shed light on the state of HTTPS implementation in libraries, and to suggest ways in which libraries can evaluate and improve application security so that they can better protect the confidentiality of PII about library patrons.

The remainder of this paper is organized as follows: the second section discusses previous work on the topic of confidentiality as it pertains to librarianship and cybersecurity. The testing methods used to evaluate HTTPS implementation are described in the third section. The fourth section describes the research method, and the fifth section presents the empirical results. The sixth section discusses the findings, and section seven explains the limitations of the study and offers suggestions for future research. Finally, the conclusion summarizes the key finding and contributions of the paper.

2. Literature Review

The research begins with a survey of the literature on the topic of confidentiality as it pertains to patron privacy; the impact of information technology on libraries; and the use of Hypertext Transport Protocol Secure (HTTPS) as an security control to protect the confidentiality of patron data when it is transmitted over the public Internet. While there is ample literature on the topic of patron privacy, there appears to be

a lack of empirical studies that measure the use of HTTPS to protect the privacy of data transmitted to and from patrons when they use library Web applications.

2.1. The Primal Importance of Patron Privacy

Patron privacy has long been one of the most important principles of the library profession in the United States. As early as 1939, the Code of Ethics for Librarians explicitly stated, "It is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons" (American Library Association, 1939). The concept of privacy as applied to personal and circulation data in library records (Crooks, 1976; Harter & Busha, 1976; Fouty, 1993) began to appear in the library literature not long after the passage of the U.S. Privacy Act of 1974.

Today, the American Library Association (ALA) regards privacy as "fundamental to the ethics and practice of librarianship" (ALA, 2008), and has formally adopted a policy regarding the confidentiality of personally identifiable information (PII) about library users, which asserts, "confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf" (ALA, 1991). This policy affirms language from the ALA Code of Ethics, and states that confidentiality extends to "information sought or received and resources consulted, borrowed, acquired or transmitted," including database records, reference interviews, circulation records, interlibrary loan records, and "other personally identifiable uses of library materials, facilities, or services" (ALA, 1991). In more recent years, the ALA has further specified that right of patrons to privacy applies to any information that can link "choices of taste, interest, or research with an individual" (ALA, 2002).

2.2. The Impact of Information Technology on Patron Privacy

Researchers have studied the impact of information technology on patron privacy for several decades. Early research by Harter (1977) and Machovec (1988) discussed the data privacy challenges arising from the use of automated systems in the library, and the associated ethical considerations for librarians who create, view, modify, and use patron records. Fouty (1993) addressed issues regarding the privacy of patron data contained in library databases, arguing that online patron records provide more information about individual library users, more quickly, than traditional paper-based files. Anderson, Agnew, and Miller (1996) presented a hypothetical case involving the transmission of an obscene email from a library computer, and an ensuing FBI inquiry, as a method of examining privacy issues that arise from patron Internet use at the library. And Merry (1996) pointed to the potential for violations of patron privacy brought about by tracking of personal information attached to electronic text supplied by publishers.

The general consensus from the literature, as articulated by Fifarek (2002), is that technology has given rise to new privacy challenges, and that the adoption of technology in the library has outpaced efforts to maintain patron privacy. This sentiment was echoed and amplified by former ALA president John Berry, former ALA president, who commented that there are "deeper issues that arise from the impact of converting information do digitized, online formats" and critiqued the library profession for having "not build protections for such fundamental rights as those to free expression, privacy, and freedom" (Berry, 2002). The ALA itself affirmed these findings and validated much of the prevailing research in a report from the Library Information Technology Association, which concluded, "User records have also expanded beyond the standard lists of library cardholders and circulation records as libraries begin to use electronic communication methods such as electronic mail for reference services, and as they provide access to computer, web and printing use" (ALA, 2000a.).

In more recent years, library systems have made increasing use of network communication protocols such HTTP, and focus of the literature has shifted towards Internet technologies in response to the growth of trends such as cloud computing and Web 2.0. Mavodza (2012) characterizes the relevance of cloud computing as "unavoidable" and expounds on the ways in which Software-as-a-Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) and other cloud computing models "bring to the

forefront considerations about...information security [and] privacy…that the librarian has to be knowledgeable about." Levy (2012) and Bérard (2013) caution that next-generation library systems and web-based solutions are "a breakthrough but need careful scrutiny" of security, privacy, and related issues such as data provenance (i.e., where the information is physically stored, which can potentially affects security and privacy compliance requirements).

2.3. Protecting Patron Privacy in the "Library 2.0" Era

"Library 2.0" is an approach to librarianship that emphasizes engagement and multidirectional interaction with library patrons. Although this model is "broader than just online communication and collaboration" and "encompasses both physical and virtual spaces" (Stephens, 2011), there can be no doubt that "Library 2.0 is rooted in the global web 2.0 discussion" (Zimmer, 2013), and that libraries have made increasing use of web 2.0 technologies to engage patrons. The Library 2.0 model disrupts many traditional practices for protecting privacy, such as limited tracking of user activity, short- term data retention policies, and anonymous browsing of physical materials. Instead, as Zimmer (2013) states, "the norms of Web 2.0 promote the open sharing of information—often personal information—and the design of many Library 2.0 services capitalize on access to patron information and might require additional tracking, collection, and aggregation of patron activities." As the ALA (2000b) cautioned in their study on privacy and confidentiality, "Libraries that provide materials over websites controlled by the library must determine the appropriate use of any data describing user activity logged or gathered by the Web server software." The dilemma facing libraries in the Library 2.0 era, then, is how to appropriately leverage user information while maintaining patron privacy.

Many library systems require users to validate their identity through the use of a username, password, PIN code, or another unique identifier for access to their library circulation records and other personal information (LITA, 2000). However, several studies (LITA, 2000; Dixon, 2008; Delozier, 2012) suggest the authentication process itself spawns a trail of personally identifiable information about library patrons that must be kept confidential. There is discussion in the literature (Breeding, 2006) about the value of using HTTPS and SSL certificates to protect patron privacy and build a high level of trust with users, and general awareness about importance of encrypting communications that involve sensitive information, such as "payment for fines and fees via the OPAC" or when "patrons are required to enter personal details such as addresses, phone numbers, usernames, and/or passwords" (Breeding, 2006). However, as Breeding observed, many OPACs and other library automation software products "don't use SSL by default, even when processing these personalization features." These observations call library privacy practices into question, and are concerning since "hackers have identified library ILSs as vulnerable, especially when libraries do not enforce strict system security protocols" (Engstrom, 2006).

One of the challenges facing libraries is the perception that "a library's basic website and online catalog functions don't need enhanced security" (Breeding, 2006). This belief may be based on the historical practice of using HTTPS selectively to secure "sensitive" information and operations such as user authentication. But in recent years, it has become clear that selective HTTPS implementation is not an adequate defense. The Electronic Frontier Foundation (EFF) cautions, "Some site operators provide only the login page over HTTPS, on the theory that only the user's password is sensitive. These sites' users are vulnerable to passive and active attacks" (EFF, 2011).

2.4 HTTP Exploits

Web servers typically generate unique session token IDs for authenticated users and transmits them to the browser, where they are cached in the form of cookies. -Session hijacking is a type of attack that "compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the web server," often by using a network sniffer to capture a valid session ID that can be used to gain access to the server (OWASP, 2011). Session hijacking is not a new problem, but the release of the Firesheep attack kit increased awareness about the inherent insecurity of HTTP and the need for

persistent HTTPS (Butler, 2010 Watters, 2011). In the wake of Firesheep's release and several major security breaches, former Sen. Charles Schumer, in a letter to Yahoo!, Twitter, and Amazon (Info Security Magazine, 2011), characterized HTTP as a "welcome mat for would-be hackers" and urged the technology industry to implement better security as quickly as possible. These and other events prompted several major site operators, including Google, Facebook, PayPal, Twitter, to switch from partial to pervasive HTTPS. Today these sites transmit all virtually Web application traffic over HTTPS. Security researchers from these companies, as well as from several standards organizations (EFF, IETF, OWASP) have shared their experiences and recommendations to help other website operators implement HTTPS effectively. These include encrypting the entire session, avoiding mixed content, configuring cookies correctly, using valid SSL certificates, and enabling HSTS to enforce HTTPS.

3. Testing Techniques Used to Evaluate HTTPS Implementation

There is little or no evidence in the literature that libraries are aware of the associated vulnerabilities, threats, or risks, or that researchers have evaluated the use of HTTPS in library Web applications. However, there are many methods that libraries can use to evaluate HTTPS and SSL/TLS implementation, including automated software tools and heuristic evaluations. These methods can be combined for deeper analysis.

3.1. Automated Software Tools

Among the most widely used automated analysis software tools is SSL Server Test from Qualys SSL Labs. This online service "performs a deep analysis of the configuration of any SSL web server on the public Internet" (Qualys, 2013) and provides a visual summary as well as detailed information about authentication (certification and certificate chains) and configuration (protocols, key strength, cipher suites, and protocol details). Users can optionally post the results to a central "board" that acts as a clearinghouse for identifying "insecure" and "trusted" sites. Another popular tool is SSLScan, a command-line application that, as the name implies, quickly "queries SSL services, such as HTTPS, in order to determine the ciphers that are supported" (Sourceforge, 2014). However, these tools are limited in that they only report specific types of data and do not provide a holistic view of HTTPS implementation.

3.2. Heuristic Evaluations

In addition to automated software tools, librarians can also use heuristic evaluations to manually inspect the gray areas of HTTPS implementation, either to validate the results of automated software or to examine aspects not included in the functionality of these tools. One example is HTTPSNow, a service that lets users report and view information about how websites use HTTPS. HTTPSNow enables this activity by providing heuristics that non-technical audiences can use to derive a relatively accurate assessment of HTTPS deployment on any particular website or application. The project documentation includes descriptions of, and guidance for identifying, HTTP-related vulnerabilities such as use of HTTP during authenticated user sessions, presence of mixed content (instances in which content on a web page is transmitted via HTTPS while other content elements are transmitted via HTTP), insecure cookie configurations, and use of invalid SSL certificates.

4. Research Methodology

A combination of heuristic and automated methods were used to evaluate HTTPS implementation in a public library Web application to determine how many security vulnerabilities exist in the application, and assess to the potential privacy risks to the library's patrons.

4.1. Research Location

This research project was conducted at a public library in the western United States (U.S.) that we call XYZ Public Library (XPL). This library was established in 1908. It employs 90 staff and approximately 40 volunteers. In addition, it has approximately 91,000 cardholders. As part of its operations, XPL runs a

public-facing website and an integrated library system (ILS) that includes an OPAC with personalization for authenticated users.

4.2. Test

To conduct the test, a valid XPL library patron account was created and used to authenticate the researcher for access to account information and personalized features of XPL's OPAC. Next, the Google Chrome web browser was used to visit XPL's public-facing website. A valid patron name, library card number, and eight-digit PIN number were then used to gain access to online account information. Several tasks were performed to evaluate HTTPS usage. A sample search query for the keyword "recipes" was performed in the OPAC while logged in. The description pages for two of the resources listed in the search engine result page (one printed resource and one electronic resource) were clicked on and viewed. The electronic resource was added to the online account's "book cart" and the book cart page was viewed.

During these activities, HTTPSNow heuristics were applied to individual web pages and to the user session as a whole. The web browser's URL address window was inspected to determine whether some or all pages were transmitted via HTTP or HTTPS. The URL icon in the browser's address bar was clicked on to view a list of the cookies that the application set in the browser. Each cookie was inspected for the text, "Send for: Encrypted connections only", which indicates that the cookie is secure. Individual web pages were checked for the presence of mixed (encrypted and unencrypted) content. Information about individual SSL certificates was inspected to determine their validity and encryption key length. All domain and subdomain names encountered during these activities were documented. The Google Chrome web browser was then used to access the Qualys SSL Server Test tool. Each domain name encountered was submitted. Test results were then examined to determine whether any authentication or configuration flaws exist in XPL's Web applications.

5. Results

Analysis results from the test show serious security flaws in HTTPS implementation for XPL's Web applications. The research suggests that despite legal and professional requirements to protect patron privacy, XPL has not implemented appropriate measures to secure their Web applications. These flaws are described in the sections that follow.

5.1. Use of HTTP During Authenticated User Sessions

XPL does not use HTTPS pervasively across the entire Web application. First, the homepage of XPL's website is transmitted via HTTP by default. Manually entering the URL with an "https" prefix resulted in a redirect to the unencrypted "http" page. In addition, the XPL OPAC appears to transmit some pages over HTTP and others over HTTPS. For example, when a search query is performed in the Search bar located on the patron account page, the search engine results page is sometimes served over HTTPS, and sometimes over HTTP (see Figure 1). This behavior appears to be random and is not limited to specific pages. This flaw leaves library patrons vulnerable to Firesheep-style attacks that exploit gaps in HTTPS implementation.

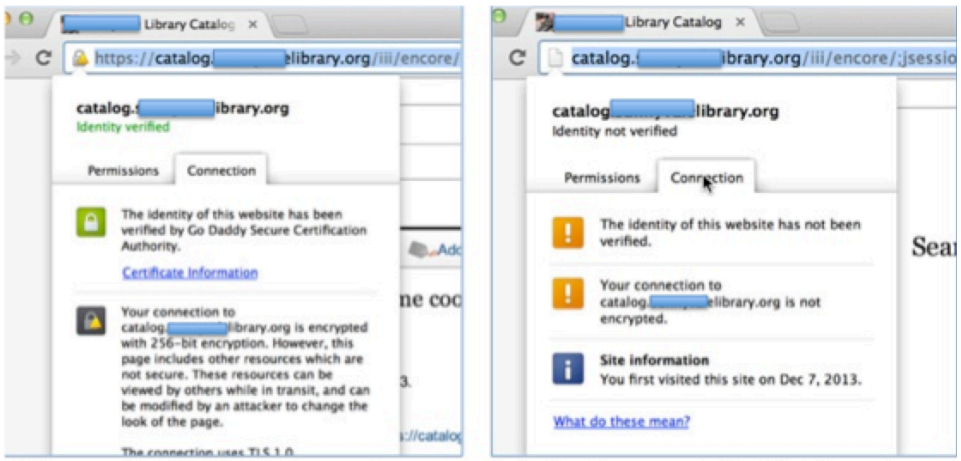

Figure 1. Results of the Library's use of HTTPS

5.2. Presence of Mixed Content

Analysis of the site did not reveal any explicit use of mixed content on the public-facing portions of the website. However, unencrypted content sources were detected on some pages of the library's online catalog. This puts patron privacy at risk because attackers can intercept the HTTP resources when an HTTPS page loads an image, iFrame, or font over HTTP, compromising the security of an otherwise secure site by enabling an attacker to exploit an insecure CSS file or JavaScript function (EFF, 2010).

5.3. Insecure Cookie Management

XPL's cookie policies are inconsistent. While one domain used for the Web application uses an JSESSION cookie that is configured to send for "secure connections only," indicating that the session ID cookie is encrypted during transmission, another domain uses an ASP.NET session ID that is configured to send for any connection, which means the session ID could be transmitted in an unencrypted format and intercepted by an attacker in order to eavesdrop on or hijack the user session.

5.4. Flawed Encryption Protocol Support

Results of the Qualys test (see Figure 2) indicate that the site does not support TLS 1.2, which means the server may be vulnerable to BEAST attacks that exploit weaknesses in earlier protocols to decrypt cookies (Ristic, 2011). In addition, the application's server platform supports SSL 2.0, which is insecure because it is subject to a "number of active attacks on its record layer and key-exchange protocol" (Wagner & Schneier, 1996).

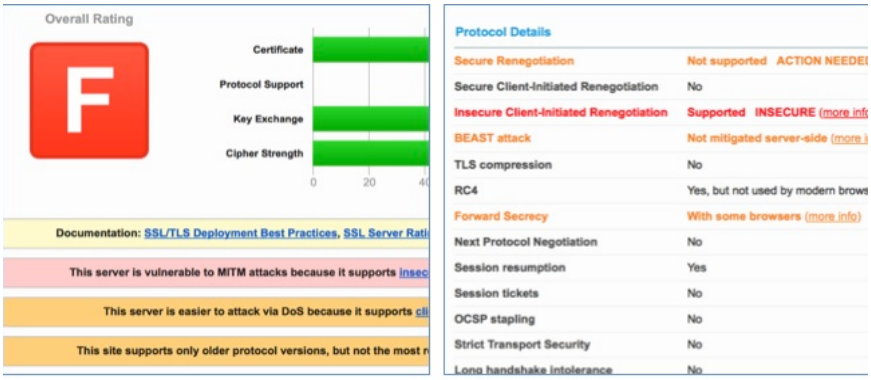

Figure 2. Qualys Scanning Service Results

6. Discussion

The results of this test suggest that XPL's Web applications possesses a number of vulnerabilities that could potentially be exploited by attackers to compromise the confidentiality of PII about library patrons, but is not surprising given the lack of research on HTTPS implementation, as well as the general consensus in the literature that technology adoption has outpaced efforts to maintain patron privacy. The vulnerabilities discovered during the testing process may be the result of uncoordinated security. The heuristic and automated tests reveal that XPL's website and ILS span across several domains. Some of these domains appear to be operated by XPL, while others appear to be part of a hosted environment operated by the ILS vendor. Based on this information, it is reasonable to conclude that XPL's ILS utilizes a "hybrid cloud" model, and that the seemingly random use of HTTPS observed in the OPAC interface during the heuristic examination may be a function of which domain handled the request.

While it seems clear that XPL needs to revisit their Web application security measures, implementing improvements to HTTPS implementation should be a straightforward process for which there is ample guidance from the security community. The latter issue, uncoordinated security, is perhaps more concerning because it is a byproduct of the cloud computing approach used to operate XPL's ILS. While libraries may have acclimated to the challenge of coordinating security measures across a distributed application, they now face the added complexity of coordinating security measures with their vendors, who themselves may also utilize additional cloud-based offerings from third parties, such as Amazon Simple Storage Service (Amazon, 2014). As cloud technology adoption increases and cloud-based infrastructures become more complex and distributed, attackers will likely attempt to find and exploit systems with inconsistent or uneven security measures, and libraries will need to work closely with information technology vendors to ensure tight coordination of security measures.

7. Limitations and Future Research

This research was performed at a public library in the western U.S. Therefore, future research is needed to study the implementation of HTTPS to increase patron privacy at other public libraries and in other parts of the U.S. and in other countries. It would also be valuable to conduct similar research at libraries of different types, including academic, law, medical, and other types of special libraries. SSL Server Test from Qualys SSL Labs and HTTPSNow were used to evaluate the use of HTTPS at XPL. The use of other evaluation techniques may generate different results.

While a major limitation of this study is the evaluation of a single public library and the implementation of HTTPS to ensure patron privacy, a next phase of research should further investigate the policies in place that are used to safeguard patron privacy. This includes security education, training and awareness programs, as well as access controls. Furthermore, library 2.0 and cloud computing are fundamental to libraries, but create risks that could impact the ability to keep patron PII safeguarded. As such, future research should evaluate the impact library 2.0 and cloud computing applications have on maintaining the confidentiality of patron information.

8. Conclusion

The library profession has long been a staunch defender of privacy rights, and the literature reviewed indicates strong awareness and concern about the rapid pace of information technology and its impact on the confidentiality of personally identifiable information about library patrons. Much work has been done to educate librarians and patrons about the risks facing them and the measures they can take to protect themselves. However, the research and experimentation presented in this report strongly suggest that there is a need for XPL and other libraries to reassess and strengthen their HTTPS implementations. HTTPS is not a panacea for mitigating Web application risks, but it can help libraries give patrons the assurance of knowing they take security and privacy seriously, and that reasonable steps are being taken to protect them. Finally, this report concludes that further research on library application security should be conducted to assess the overall state of application security in public, academic and special libraries,

with the long-term objective of enabling the ALA and other professional institutions to develop policies and best practices to guide the secure adoption of Library 2.0 and cloud computing technologies within a socially connected world.

References

Amazon Web Services (2014). Amazon Simple Storage Service (S3) – Cloud Storage. Retrieved from http://aws.amazon.com/s3/

American Library Association (1939). *History of the Code of Ethics: 1939 Code of Ethics for Librarians.* Retrieved from http://www.ala.org/Template.cfm?Section=History1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=8875

American Library Association (1991). Policy concerning Confidentiality of Personally Identifiable Information about Library Users. Retrieved from http://www.ala.org/offices/oif/statementspols/otherpolicies/policyconcerning

American Library Association (2000). *Appendix*. Retrieved from http://www.ala.org/lita/involve/taskforces/dissolved/privacy/appendix

American Library Association (2000). *Final Report*. Retrieved from http://www.ala.org/lita/about/taskforces/dissolved/privacy

American Library Association (2002). *Privacy: An Interpretation of the Library Bill of Rights*. Retrieved from http://www.ala.org/Template.cfm?Section=interpretations&Template=/ContentManagement/ContentDisplay.cfm&ContentID=83534#6

American Library Association (2008). *Code of Ethics of the American Library Association*. Retrieved from http://www.ala.org/advocacy/proethics/codeofethics/codeethics

Anderson, A. , Agnew, G. , & Miller, R. (1996). The sex files. *Library Journal, 121*(2), 54.

Bérard, R. (2013). Next generation library systems: new opportunities and threats. *Bibliothek, Forschung und Praxis, 37*(1), pp. 1-144.

Berry, J. (2002). Digital democracy: not yet! *Library Journal, 125*(1), 6.

Breeding, M. (2006). *Building trust through secure web sites*. Computers in Libraries, vol. 25(6).

Butler, Eric (2010). *Firesheep*. Retrieved from http://codebutler.com/firesheep/

Crooks, J. (1976). Civil Liberties, libraries, and computers. *Library Journal, 101*. 482-487.

Delozier, E. (2012). Anonymity and authenticity in the cloud: issues and applications. *OCLC Systems and Services: International Digital Library Perspectives*, vol. 29(2), p. 65-77.

Dixon, P. (2008). Ethical issues implicit in library authentication and access management: risks and best practices. *Journal of Library Administration*, vol. 47(3), p. 141-162.

Electronic Frontier Foundation (2010). *How to Deploy HTTPS Correctly.* Retrieved from https://www.eff.org/https-everywhere/deploying-https

Electronic Frontier Foundation (2011). *'HTTPS Now' Campaign Urges Users to Take an Active Role in Protecting Internet Security*. Retrieved from https://www.eff.org/press/archives/2011/04/19-0

Engstrom, B. (2006). Evaluating patron privacy on your ils: how to protect the confidentiality of your patron information. *AALL Spectrum; April 2006*, vol. 10(6), p4-19.Fouty, K. (1993). Online patron records and privacy: Service vs security. *Journal of Academic Librarianship*, *19*, 289-293.

Fifarek, (2002). Technology and privacy in the academic library. *Online Information Review, 26*(6), 366–374.

Fouty, K. (1993). Online patron records and privacy: Service vs security. *Journal of Academic Librarianship*, *19*, 289-293.

Harter, S. (1977). Privacy and security in automated personal data systems. *An Intellectual Freedom Primer* (ed. Charles H. Busha). Littleton, CO: Libraries Unlimited. pp. 90-91.

Harter, S. , & Busha, C. (1976). Libraries and privacy legislation. *Library Journal, 101*. 475-481.

Info Security Magazine (2011). *Senator Schumer: Current internet security "welcome mat for would-be hackers.* Retrieved from http://www.infosecurity-magazine.com/view/16328/senator-schumer-current-internet-security-welcome-mat-for-wouldbe-hackers/

Ismail, R. , & Zainab, A. (2013). Assessing the status of library information systems security. *Journal of Librarianship & Information Science*, *45*(3), 232-247.

Levy, R. (2013). Library in the cloud with diamonds: A critical evaluation of the future of library management systems. *Library Hi Tech News, 30*(3), 9-13.

Machovec, G.S. (1988). Data security and privacy in the age of automated library systems. *Information Intelligence, Online Libraries and Microcomputers, 6*(1).

Mavodza, J. (2012). The impact of cloud computing on the future of academic library practices and services. *New Library World*, vol. 114(3/4).

Merry, L. (1996). Hey, look who took this out!--privacy in the electronic library. *Journal of Interlibrary Loan, Document Delivery & Information Supply, 6*(4), 35-44.

Open Web Application Security Project (2011). *Session Hijacking Attack*. Retrieved from https://www.owasp.org/index.php/Session_hijacking_attack

Open Web Application Security Project (2013). *Periodic Table of Vulnerabilities - Cookie Theft/Session Hijacking*. Retrieved from https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Cookie_Theft/Session_Hijacking

Open Web Application Security Project (2013). *Session Management*. Retrieved from https://www.owasp.org/index.php/Session_Management

Qualys SSL Labs (2013). *SSL/TLS Deployment Best Practices*. Retrieved from https://www.ssllabs.com/projects/best-practices/

Ristić, I. (2011). Mitigating the beast attack on tls. Retrieved from https://community.qualys.com/blogs/securitylabs/2011/10/17/mitigating-the-beast-attack-on-tls

Ristić, I. (2013). *SSL/TLS Deployment Best Practices*. Retrieved from https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf

SourceForge (2014). SSLScan - Fast ssl scanner. Retrieved from http://sourceforge.net/projects/sslscan/

Stephens, Michael (2011). *The Hyperlinked Library: a TTW White Paper*. Retrieved from http://tametheweb.com/2011/02/21/hyperlinkedlibrary2011/

Wagner, D., & Schneier, B. (1996). Analysis of the SSL 3.0 protocol. *Electronic Commerce Proceedings, Second USENIX Workshop on*, 29-40.

Watters, A. (2011). *Zuckerberg's Page Hacked, Now Facebook To Offer "Always On" HTTPS*. Retrieved from http://readwrite.com/2011/01/26/zuckerbergs_facebook_page_hacked_and_now_facebook

Zimmer, M. (2013). Patron Privacy in the" 2.0" Era. Journal of Information Ethics, 22(1), 44-59.