SharePoint Communication Protocol Hardening

Robert Underwood

ECU

Fundamental Network Security

ICTN6865

Dr. Lunsford

November 28, 2014

Abstract

SharePoint Communication Protocol Hardening will discuss the details related to sever to server communication within the SharePoint communication schema. This paper will describe the types of protocols that SharePoint is capable to using with an emphasis on NTLM communication. Within the discussion of NTLM communication an in depth review of the NTLM protocols the NTLM benefits will be reviewed and the current risk regarding NTLM vulnerabilities. In the analysis of the NTLM vulnerabilities this paper will discuss current mitigation techniques used to harden the NTLM communication protocols.

SharePoint Communication Protocol Hardening

SharePoint is a product of Microsoft office and used as a tool for Knowledge Management. The key to SharePoint design is understanding the fundamentals of Knowledge Management and although this paper will not expand on these Knowledge Management concepts they are the basis for every configuration decision made around every aspect of SharePoint. From hardware selection to information taxonomies it all starts, and is based, on a Knowledge Management requirement. As a tool for Knowledge Management SharePoint helps the fundamental ideas associated within the Knowledge Management processes of locating, organizing, transferring, and using information as Duffy explains in her journal paper (Duffy, 2000). Once installed and configured SharePoint allows user to create an intranet platform where a user can make web pages, web parts, libraries, lists, and many other content areas where information can be organized, located, transferred, and used (Microsoft Office, n.d.).

Information Security

Understanding the uses of SharePoint is important to how security is applied to information, not all information is open to public viewing or everyone in the company, some types of information needs restricted access. SharePoint allows users to create security groups that give read, write, and edit functionality to information. When information is organized with information architecture the access to important information becomes easy for users to find (King & Jannik, 2005). SharePoint can be built on one server or on may servers called a farm, this paper will address the farm configuration due to server to server communications that take

place for several pieces of SharePoint such as the database, index, and front end server communications.

SharePoint's security model allows for the fundamental security model of confidentiality, integrity, and availability. These concepts are defined by basic security principles in the security industry and explained in the Certified Information Privacy Professional, CIPP, guide website (CIPPS Guide, 2010) and defined as:

1) **Confidentiality.** Like privacy confidentiality means that information is only available to the appropriate parties and confidential information is not disclosed to people who do not have the rights to view the information. Ensuring confidentiality means the information is organized in a restrictive manner to authorized users. SharePoint ensures confidentiality by using security groups to allow users to organize user information in a way to create restrictive locations that lock out unwanted viewers. In addition SharePoint offers a reporting method that audits users' access to determine if restricted users have viewed information within a restricted area.
2) **Integrity.** The integrity of information refers to the certainty that the information is not changed or destroyed by unauthorized users after submission. SharePoint allows users to set permissions on information to prevent users from viewing. SharePoint allows user to set versioning on information so if information has been changed the current version shows who made the change and a copy of the original is set for retrieval in the event that unauthorized changes were made. In addition SharePoint allows users to set alarms and email messages to information owners should any change be made to the information.

3) **Availability.** Retrieving information when it is needed is called availability. Keeping information available means that the systems that host the information are ready and available at a specific time. Many systems allow 24 hour access and have continuity plans to restore access if the system should fail, some of these systems have High Availability which means when the system fails there are additional systems in place that ensure the failure does not interrupt service, as stated by CISCO with their High Availability designs (CISCO, n.d.).

With the CIA model presented by (CIPPS Guide, 2010) users can feel confident that their information in the system is safe and secure and with the SharePoint functions that provide the service required by the CIA model SharePoint users can be confident that their information in the SharePoint systems is also safe and secure.

SharePoint System Design

SharePoint farm design includes an index server, database server, application server, query severs, and a front end server.

Index Server. The index server hosts the indexes formed from the information stored in SharePoint by the users. SharePoint reserves this index to assist the user with search queries by searching the user key words against the index which links to stored information. This technique accelerates the information retrieval methodology in SharePoint.

Database Server. The database server, Microsoft SQL, is where all the information is stored to operate SharePoint and to manage user information. The average user or even a power user does not need to have special knowledge about Microsoft SQL

to use SharePoint. Although understanding the principles of database design are very helpful when designing information hierarchies and work processes through standard SharePoint designs.

Application Server. The application hosts applications like SharePoint central administration, search, and crawl services. This server performs separate operations on users' requests so that the request can be processed in the background with a separate resource. This offloads some of the traffic burden within the SharePoint system.

Front End Server. As one of the most important pieces of a SharePoint farm the Front End Server is a Web front end the gateway from the internet to the farm. This communication channel from the internet, HTTP or HTTPS, is managed by the Microsoft's Internet Information Services, IIS. The Front End Sever manages the all the user traffic in and out of SharePoint.

SharePoint Dependencies

SharePoint depends on many resources outside the SharePoint application that are controlled by an operating system. SharePoint is designed to operate within Microsoft's operating systems (Microsoft, n.dc.) which shows SharePoint utilizes more than one hundred types of protocols used to run services managed by SharePoint, such as, indexing, searching, database communications as seen in the physical schema (Microsoft Developer Network, n.d.). As SharePoint sends traffic across the internet and even from server to server SharePoint uses, by default, an authentication protocol by default called NTLM, which will be a focus of this paper. SharePoint can also be configured to work with a stronger type of authentication called Kerbros

which has a stronger encryption method than Microsoft's New Technology LAN Manager, NTLM (Cherny, 2009).

Kerbros encryption for SharePoint seems to be a viable solution but there are issues that occur during a Kerbros communication that can cause Kerbros to fail and when Kerbros fails, in most cases, Kerbros will default back to NTLM (Microsoft Technet, n.d.a, p. 1). When this occurs there is no indication, Alarm, by SharePoint to the user, administrator, or anyone else that the error has taken place therefore putting the system in a state that may or may not be secure. To assure the systems are secure we must make sure the SharePoint farm is operating correctly as given by the setup manual by Microsoft (Microsoft Technet, n.d.e). Once NTLM is operating correctly we can review vulnerabilities of NTLM and take mitigative action to prevent exploitation therefore ensuring maximum security in NTLM and if Kerbros fails.

NTLM

According to Microsoft NTLM was developed by Microsoft as a protocol to manage authentication to network devices from systems that utilized Microsoft operating systems and uses credentials to manage authentication as described by Microsoft as "NTLM credentials are based on information obtained during the interactive logon process and consist of a domain name, a user name, and a one-way hash of the user's password. NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials.

Interactive NTLM authentication over a network typically involves two systems: a client system, where the user is requesting authentication, and a domain controller, where information

related to the user's password is kept. Non-interactive authentication, which may be required to permit an already logged-on user to access a resource such as a server application, typically involves three systems: a client, a server, and a domain controller that does the authentication calculations on behalf of the server." (Microsoft, n.d.a, para. 3).

NTLM Methodology

If a user follows the installation guilds for the operating system and SharePoint correctly the NTLM functionality should be working at expected. With all baseline service in place there still exists a slight problem, the NTLM method has known security issues that can be exploited. The NTLM exploits are based on an algorithm used to by the NTLM method which is depicted in figure 1.

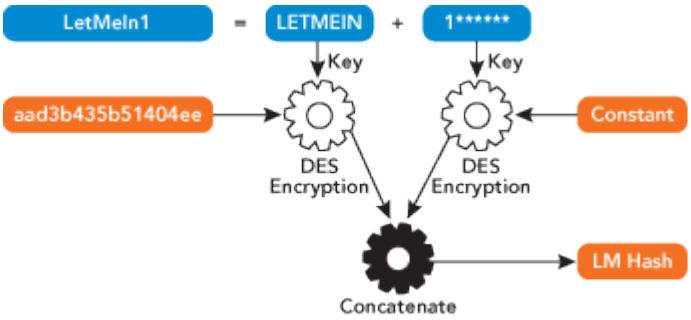

Figure 1. Then NTLM Method (Johansson, n.d., figure 1)

The first weakness in the NTLM algorithm according to Johansson (Johansson, n.d., p. 1) is that all lowercase characters are forced to uppercase. What this does is reduce the number of the characters in the pool, a smaller pool means the password will be easier to guess as used in specific account attacks where "The attacker targets a specific account and submits password guesses until the correct password is discovered. The standard countermeasure is an account lockout mechanism, which locks out access to the account after a number of failed login attempts. Typical practice is no more than five access attempts." (Stallings, 2011, p. 74). Since

the system generates the password for this method it would seem appropriate for the developer to create an exceptionally long password, say thirty characters, so that even in the event the pool to hack is smaller the sheer number of increased characters would increase the password complexity to a point that it would take years to hack one password (Todd, 2012). Unfortunately this will not work as well as we would imagine because of the second algorithm flaw.

The second weakness according to Johansson (Johansson, n.d., p. 1) the NTLM algorithm involves splitting the password into two seven character chunks which defeats the purpose of creating a long password that was mentioned as a mitigation in the first weakness. By splitting the password into seven character chunks an attacker has a much small attack surface and a much better probability of success reducing password complexity by many powers of magnitude. Johansson (n.d.) states that Microsoft has updated NTLM to NTLM2 and although it uses a different algorithm the password strength is still lacking. This is due to the password length which is variable and includes the server name, share name, and a few other constants. Using this known information that can be obtained by an attacker the attacker has a significant advantage in reducing the time to crack the password as seen in those types of attacks that are used in dictionary attacks (Stallings, 2011, p. 74).

Hardening NTLM

To harden NTLM or NTLM2 the developer, Microsoft, could add a salt pad in the routine and increase the password complexity as seen in Unix systems and is mentioned by Stallings (2011, p. 75). This seems like a better solution but a user cannot change the methodology for it is owned by Microsoft so with the control out of the hand of the user further steps are needed to secure the NTLM methodologies.

Understanding that NTLM and NTLM2 work within the domain of a network and are handled by the Open System Interconnection Model, OSI, is where a user can apply techniques that can enhance the standard NTLM or NTLM2 methods.

The OSI Model

To understand how the OSI model and the NTLM methods work together the user should have some understanding of the OSI model. The OSI model starts with the Ethernet protocol which is the network Physical Link and the Data Link layer of communication and it defined in the OSI model layer 1 and layer 2. The OSI layer 1 is the physical network layer and this layer moves the bit stream over the network medium to the receiving device and the visa versa, providing a sending and receiving mechanism for communication.

The OSI layer 2 is the Data Link Layer which sets up a link across the Physical Layer 1on the network by establishing network packets within network frames. This layer has two sub-layers the Logical Link Control sub layer and the Media Access Control sub layer (Day & ZIMMERMANN, 1983). With these two layers the data stream is broken down into chunks of data, packets, and wrapped into a frame and sent across the network medium to its destination (McIlroy, 2004, p. 1). The frame has the following Ethernet protocol design in figure 2.

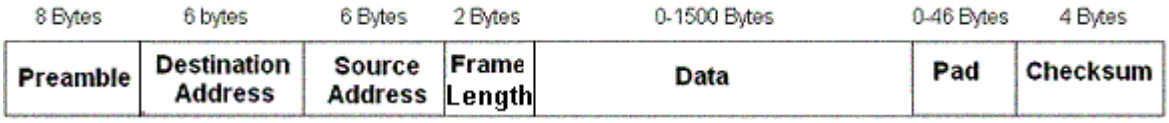

Figure 2. Ethernet frame (McIlroy, 2004, p. 1)

Once the connection has been established these frames are sent across the network and the number of frames and the time it takes to send the data is what equates to the bandwidth.

Once the frames have been moved across the medium the network gives up the data stored in the layer 2 segment to the receiving system. At this point in time the physical network connection and transport system have been established but what about all the broken up data stuffed into packets.

Addressing the Data

To transport the data to the correct location the OSI model provides a layer called Network Layer 3. This layer provides all the addressing from the sender and receiver for the data delivery, referring to figure 1, the addressing is contained within the second set of bits six bits as seen in the diagram, which is reserved for the addressing and controlled by this OSI Network Layer 3 (Day & ZIMMERMANN, 1983). There is an addressing protocol used by the Network Layer 3 where the addressing schema is called the Internet Protocol, this protocol uses four blocks of numbers where each block contains one to three numbers from zero to two hundred fifty five (255), for example, 0.0.0.0 or 255.255.255.255. Each set of numbers represent an addressing schema that help networks deliver data from one machine to another ("What is an IP?," n.d., p. 1).

Data Packets

Since the communication methodology is defined into frames and the data is transported in the frame defined as packets there must be some system that defines packets so the data which is represented by the packets can be maintained. When the data is deconstructed into packets the data becomes unusable until the packets reconstruct the data on the receiving device which leads us to the OSI model layer 4 the Transport Layer.

In this layer the data is put into packets and marked with a sequence for reconstruction when the frame reaches its destination in addition error checking data is included in the frame in the form of a check sum which is included in the last four bytes of the frame, see figure 1 (Day & ZIMMERMANN, 1983).

Make the Session

During a session, the time the physical network and logical network are connected for the purpose of transmitting data, the OSI Layer 5 which is the Session Layer, sets up, maintains, and terminates the network links between destination devices. This layer provides an authentication method during the connection phase of a transmission in addition to monitoring the connection for interruption and if a disconnection should occur at reconnect method is activated and re-establishes the connection (Rouse, N.D., p. 1).

Operating System Communication

The network communication depends on an operating system so the data transferred can be moved to a usable location on a receiving device. The OSI model Layer 6, the Presentation Layer, is the layer that provides the handoff from network data to the device. The Presentation Layer provides a translation of data from the operating system to the network so the data can be transmitted. Once the data is transmitted to the receiving device the Presentation Layer translates the data from the network to a format the operating system can utilize (Rouse, N.D., p. 1).

Communication Between Apps and OS

Once the Presentation Layer delivers the data to the operating system the operating system needs to know which application has requested the information and what format to deliver the data in. Additionally the application needing to know what data was sent or requested so it can act upon the data. This OSI model is Layer 7, the Application Layer is layer that contains the directions for the operating system to start a communication session, it defines what data format will be sent, and what data format the device expects to receive (Rouse, N.D., p. 1).

OSI Model View

The OSI model is made up of seven layers of communication protocols that are a standard for the current network communications with each layer providing a special function that helps establish, maintain, transport data, translate data, and terminate data. The Escotal.com organization has produced a diagram that is very helpful to understand the interworking of OSI layers shown in figure 3. Although the diagram displayed in figure 3 contains more information than this paper has defined the foundational sever layers are listed in overview and are shown in relation to each other which is helpful for understand the interface with NTLM methodologies.

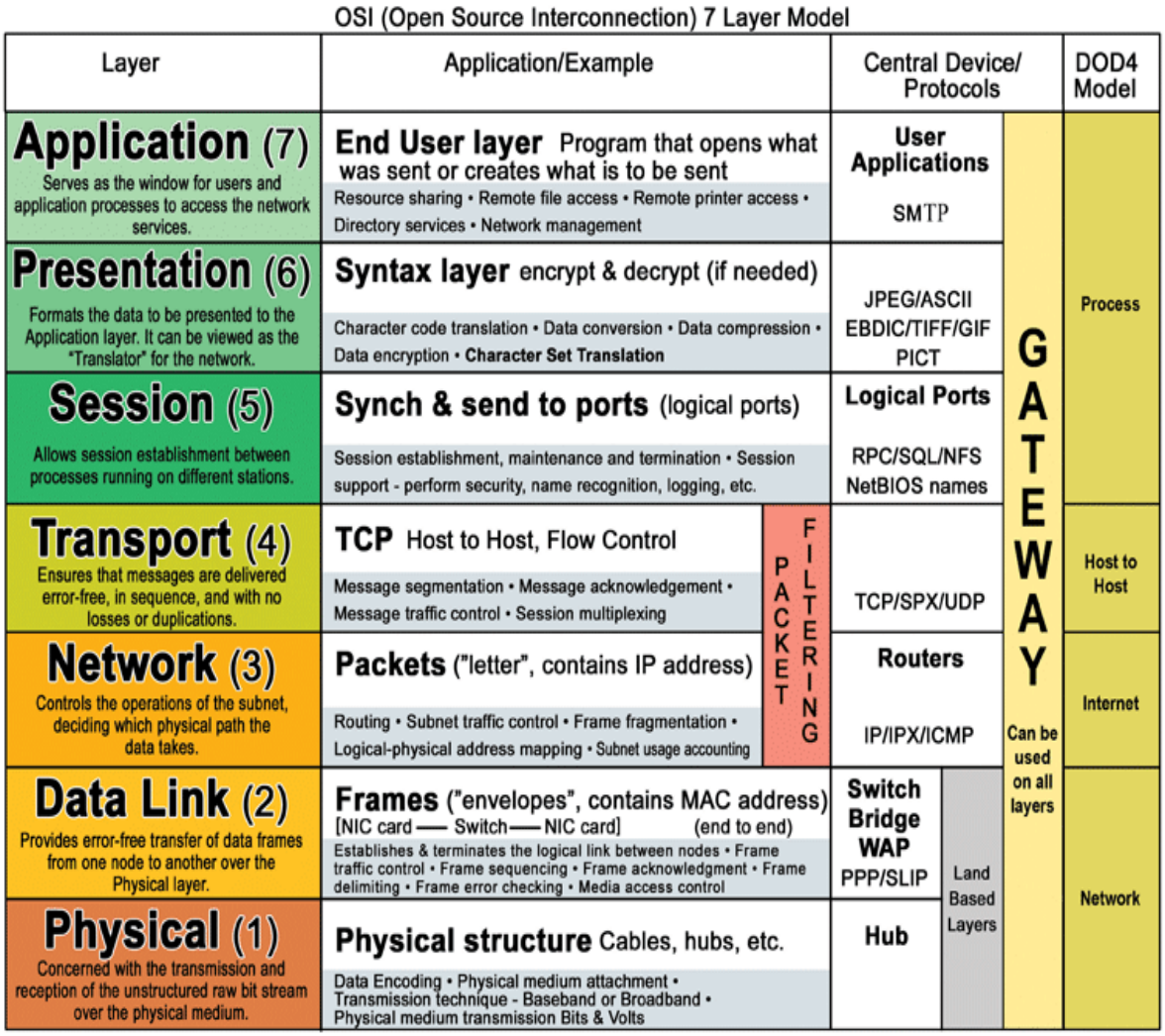

Figure 3. OSI Model 7 Layers (Escotal.Com, 2013, p. 1)

Using the OSI model we can see all the protocols that manage the network therefore if we can secure the OSI layers that the NTLM or NTLM2 depend upon, then we can make it much harder for an attacker to attack NTLM or NTLM2.

Network Isolation

The first step a user can take to help NTLM methods, let NTLM methods mean from this point forward NTLM or NTLM2, a user can setup a VLAN and only let the traffic between SharePoint servers run within this environment. The VLAN will isolate the SharePoint farm by segmenting the network traffic in a small separate network that only SharePoint servers will communicate, creating a private network (Microsoft Technet, n.d.b) depicted in figure 4, this isolation technique will secure the first three layers of the OSI model Physical Layer 1, Data Link Layer 2, and Network layer 3.

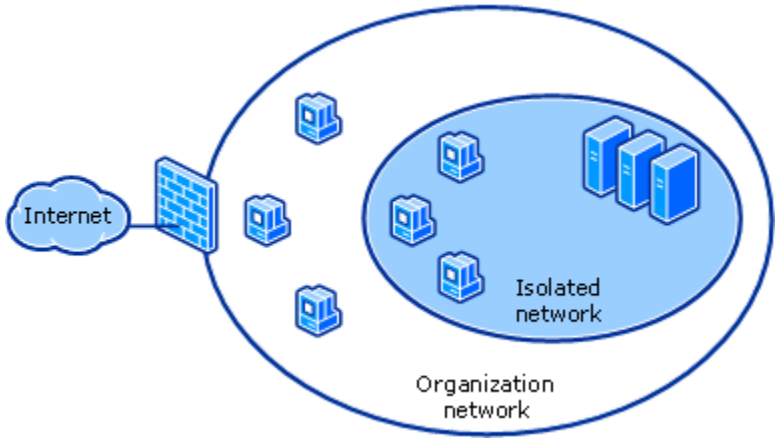

Figure 4. Isolated Network (Microsoft Technet, n.d.b)

An additional technique to securing NTLM methods is to create SharePoint user groups in the Active Directory schema which will control which users are let into SharePoint, which prevents unauthorized users from gaining access to SharePoint. When users request access they will need to authenticate against the domain before they allowed access to the organizational network. Once within the network to access SharePoint an additional check for access to the SharePoint Group in Active Directory is checked to determine whether a user is a member of the SharePoint user group. Another benefit of Active Directory is Group Policy that manages configurations setting with the operating system such as password lockout, password length, and

other configuration setting that restrict users. These settings assure that users systems comply with important security settings under the control of the operating system. Microsoft gives a great example of how this would work in the given scenario. “With group-specific server isolation, the isolated network consists of the server computers and the group of authorized domain member client computers… you can configure group-specific Server Isolation settings so that a server that contains sensitive medical information allows secure communications only with computers that meet the following criteria:

a. They are domain members.

b. They are members of the Confidential Medical Active Directory security group.” This demonstrates what Group Policy can achieve (Microsoft Technet, n.d.b).

Additionally add to the SharePoint environment and operating systems updates and security patches recommended by Microsoft (Technet, n.d.b) the isolated system should be security within the definitions set by Microsoft. With the all the for mentioned techniques the system will be meet the CSI security requirement on the OSI layers on the Transport Layer 4, Session Layer 5, Presentation Layer 6, and Application Layer 7.

The next layer of network to isolate is the organizational domain as shown in figure 4 is shown as the outer network layer, which is shown in figure 4 bordering the SharePoint isolated network. A firewall can be configured to add an additional layer of isolation limiting only those domains that are trusted such as organization defined domains.

To add another layer of protection within the organizational domain would be to add intrusion detection software, anti-virus, anti-spy war, and other malicious software deterrents. Another precaution would be to add certificates to each of the servers and to IIs configuration for HTTPS traffic on port 334 (Microsoft Technet, n.d.b). Configuring traffic for the database is slightly different but covered by the article by Microsoft (Microsoft Technet, n.d.b).

In Review

Securing the information with SharePoint meets all the CIA security requirements with the flexibility to users to setup their own model. The installation and configuration of SharePoint depends is best setup on Kerbros but the inherent flaw of defaulting to NTLM methods mean we have to take security precautions to harden the NTLM methods. The NTLM methods are designed by Microsoft and are limited to the user configuration to increase security so we need to look further into the stack of the OSI model to influence the network configuration to so that the NTLM methods can be address at a lower level.

By implementing a VLAN we can isolate SharePoint traffic to its own private network that will restrict unwanted traffic which secures the OSI model of Physical Layer 1, Data Link Layer 2, and Network Layer 3. By adding Active Directory Controls, Group Policies, and SharePoint User Groups to the outer network adjacent to the SharePoint private network we can further restrict authenticated users to only the outer network and SharePoint which completes securing the OSI layers of Transportation Layer 4, Session Layer 5, Presentation Layer 6, and Application Layer 7 .

By adding firewall restrictions we can limit access to only the domains we know are trust such as those domains defined by the organization as trusted domains. By updating and patching

the operating systems and SharePoint the systems will be current with mitigations added by the manufacture to prevent exploits. And finally by adding anti-virus, intrusion detection, anti-spy ware, and other anti-malicious code programs to the system we will have mitigated the risk of attack by a large magnitude.

References

CIPPS Guide. (2010). CIA Triad. Retrieved from https://www.cippguide.org/2010/08/03/cia-triad/

CISCO. (n.d.). Design Considerations for High Availability and Scalability in Blade Server Environments. Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/white_paper_c11-553711.html

Cherny, P. (2009). *Securing External SharePoint Communications* [technical review]. Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/magazine/2009.09.insidesharepoint.aspx

Day, J. D., & ZIMMERMANN, H. (1983). *The OS1 Reference Model* [PROCEEDINGS]. Retrieved from IEEE: http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=1457043&tag=1

Duffy, J. (2000). *Knowledge management: What every information professional should know* [Information Management Journal]. Retrieved from East Carolina University Library : http://search.proquest.com.jproxy.lib.ecu.edu/docview/227759621?pq-origsite=summon

Escotal.Com. (2013). OSI 7 Layer Model. Retrieved from http://www.escotal.com/osilayer.html

Johansson, J. (n.d.). The Most Misunderstood Windows Security Setting of All Time. *Technet Magazine*. Retrieved from http://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx

King, H. J., & Jannik, C. M. (2005). *Redesigning for usability: Information architecture and usability testing for Georgia Tech Library's website* [Journaly Article]. Retrieved from

East Carolina University e-Library: http://search.proquest.com.jproxy.lib.ecu.edu/docview/209777611?pq-origsite=summon

McIlroy, R. (2004). *Ethernet*. Retrieved from http://www.dcs.gla.ac.uk/~ross/Ethernet/protocol.htm

Microsoft Developer Network. (n.d.). *SharePoint Products and Technologies Protocols Technical Documents*. Retrieved from http://msdn.microsoft.com/en-us/library/cc339473.aspx

Microsoft MSDN. (n.d.). Microsoft NTLM. Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/aa378749%28v=vs.85%29.aspx

Microsoft Office. (n.d.). What is SharePoint? Retrieved from https://support.office.com/en-us/article/What-is-SharePoint-97b915e6-651b-43b2-827d-fb25777f446f?ui=en-US&rs=en-US&ad=US

Microsoft Technet. (n.d.). Install and configure SharePoint 2013. Retrieved from http://technet.microsoft.com/en-us/library/cc262957%28v=office.15%29.aspx

Microsoft Technet. (n.d.a). *Authentication Uses NTLM instead of Kerberos*[white paper]. Retrieved from Technet: http://technet.microsoft.com/en-us/library/cc779070%28v=ws.10%29.aspx

Microsoft Technet. (n.d.b). *Introduction to Server and Domain Isolation* [white paper]. Retrieved from Technet: http://technet.microsoft.com/en-us/library/cc756066%28v=ws.10%29.aspx

Microsoft Technet. (n.d.c). Hardware and software requirements for SharePoint 2013. Retrieved November 29, 2014, from http://technet.microsoft.com/en-us/library/cc262485%28v=office.15%29.aspx#section4

Ramakrishnan, S. (2009 , April 6). Kerberos Authentication Problem with Active Directory [Blog post]. Retrieved from Microsoft Technet: http://blogs.technet.com/b/surama/archive/2009/04/06/kerberos-authentication-problem-with-active-directory.aspx

Rouse, M. (N.D.). OSI reference model (Open Systems Interconnection). Retrieved from http://searchnetworking.techtarget.com/definition/OSI

Stallings, W. (2011). *Computer Security: Principles and Practice* (2nd Edition ed.). Retrieved from Kindal Addition

Todd, D. M. (2012, 30 Aug). Password length is more beneficial than complexity. *McClatchy - Tribune Business News*. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1036943922?pq-origsite=summon

What is an IP Address? (N.D.). Retrieved from http://whatismyipaddress.com/ip-address