https://doi.org/10.48009/4_iis_2016_208-221

UNBREAKABLE: A CONCISE OVERVIEW OF CYBERSECURITY

Kristi Berg, Minot State University, kristi.berg@minotstateu.edu
Joseph N. Crawford, Minot State University, joseph.n.crawford@minotstateu.edu
Thomas Seymour, Minot State University, tom.seymour@minotstateu.edu

ABSTRACT

Security or more appropriately, cybersecurity, is the single most important service provided by any modern technology professional or organization. In recent years, cybersecurity has been at the forefront of the media cycle, with the increase in personal information and day-to-day activities being relegated to binary infrastructure, the need for security identification and development has never been greater. Yet few, if any, grasp the full spectrum of available services and more importantly, the origins and the reasons for their existence. This article examines the history of cybersecurity methodologies, thereby exposing the means by which they operate and the circumstances that mandated their development. With a full understanding of the origins of such practices, information technology professionals at all career levels can hope to build on preceding technologies, with the goal of providing an even more secure technological future.

Keywords: Cybersecurity, Hacking, Information Security

UNBREAKABLE: A CONCISE OVERVIEW OF CYBERSECURITY

When one begins to scrape the surface of cybersecurity history, it appears at first as though the entirety of the subject came into being in the late 1990s. This is mainly because of the rapid expansion of networked connections that began during this time, but is also in-part due to the government operation titled "Eligible Receiver." This government exercise seems to have shocked the industry to life and spurred the rapid development of cybersecurity products and solutions (Warner, 2012).

In actuality, cybersecurity has been a pursuit of the technology industry (particularly that of the industrial military complex) for more than a half century (Warner, 2012). As early as the mid-1960s, the National Security Agency (NSA) was thoroughly involved in the development of practical cybersecurity methodologies. In an interview conducted in 1968, then director at the NSA, Marshall Carter, bragged about the possession of a five acre storage facility that housed in excess of one hundred interconnected computers, with communicative abilities, under full control of the NSA (Warner, 2012). A revelation that came out of this same period was a report provided by Bernard Peters, the director of the RYE program, funded by the NSA, who opined that anyone who placed sensitive data on a multiprogramming system should be fully aware of the risks involved (Warner, 2012).

The open awareness of the security risks circulated by the NSA is evidence enough to infer that serious measures were being discussed and developed to mitigate these risks as early as the 1960s. Much of the focus of the era was likely centered on the physical security aspect of the science as routing protocols such as Transmission Control Protocol (TCP) and Internet Protocol (IP) were in their infancies. While it was unlikely, due to the sheer size of computers of the day, for an individual to walk out of a secured building with a machine under their shirt, the data stored on these computers, as well as the developing and highly sought after software advances they stored, were still quite vulnerable.

Much of cyber security as we know it today, in the logical sense; became a priority in the aftermath of the development of Transmission Routing Protocol in 1974. Before this time, computers operated by the NSA utilized a network protocol entitled "Network Control Protocol" or, NCP. Network Control Protocol was efficient enough to allow for broad communications to take place between computers and a main server. However, NCP had several limiting factors and was not capable of handling the "super-network" being constructed by the NSA (Blank, 2004). In 1974, the landscape changed entirely when Vint Cerf and Bob Kahn published their work "A Protocol for Packet

Network Interconnection" (Blank, 2004). The paper describes Transmission Control Protocol, which was a host-to-host package delivery protocol that allowed for guaranteed delivery of data during an information exchange between two machines (Blank, 2004). TCP kept track of the data by splitting the information into multiple "packages." After all of the packages have arrived at the other end of the communication, the receiving host utilizes TCP to put the packages back together in the proper order (Blank, 2004). TCP included many functions not available in the NCP model, including the guaranteed delivery of data (Blank, 2004). The combination of redundant pathways, hardware and software independence, low traffic overhead, and the ability to expand networks to the internetwork, made TCP the protocol of choice for the NSA, who by 1982 had made it the official network protocol of ARPANET (Blank, 2004). The 1978 addition of Internet Protocol (IP) allowed TCP/IP to lay the groundwork for the modern global Internet (Blank, 2004).

By 1990, ARPANET was abandoned and the expansion of the modern World Wide Web had begun utilizing the basic principles of TCP/IP (Blank, 2004). It was during this time that the vulnerabilities of such a vast network enterprise came to light. As the global population began to take notice of the convenience and possibilities for this brave new world, so too did the criminals; and it was not long before the very foundations of the Internet needed to be readdressed in order to prevent personal loss at a cataclysmic scale. Such preventative measures will be the focus. Any redundancy between the introductory portions of this paper have been done for the purpose of reporting such information as accurately as possible. Much of the technology utilized for cybersecurity is built upon foundations and principles that have been used for decades.

Physical Security

At the genesis of networking technologies, computer devices were communicably limited to other devices of the same manufacturer (Lammle, Network+ Deluxe Study Guide, 2012). This configuration was so restrictive that the International Organization for Standardization (ISO), created the Open Systems Interconnections (OSI) reference model (Lammle, Network+ Deluxe Study Guide, 2012). The goal of this standard was to help vendors create networking devices and software that functioned conjointly, as opposed to independently (Lammle, Network+ Deluxe Study Guide, 2012). While the standard has never fulfilled the goal of bringing every device under the umbrella of harmonious standardization, it has adopted largely as the primary architectural networking model, still utilized by modern industry professionals (Lammle, Network+ Deluxe Study Guide, 2012).

The OSI model is a layered, hierarchical representation that divides network communications into smaller, easier to understand components; which simplifies the architectural and logical processes (Lammle, Network+ Deluxe Study Guide, 2012). The model provided manufacturers a baseline for creating apparatuses that could interact with one another, while allowing for customization at one level to avoid interference at another (Lammle, Network+ Deluxe Study Guide, 2012). The representative OSI layers are as follows, according to Lammle (2012):

- Layer 7: Application – File, print, message, database and application services
- Layer 6: Presentation – Data encryption, compression and translation services
- Layer 5: Session – Dialog control
- Layer 4: Transport – End to end communication
- Layer 3: Network – Routing
- Layer 2: Data Link – Framing
- Layer 1: Physical – The physical network topology

More than providing a basic structure for interoperable networking devices, the OSI model also provided a framework for how each layer of cybersecurity should be developed (Branstad, 1987). As each layer of the OSI model is associated with a different networking service, it allowed for developers to implement solutions with more specificity (Branstad, 1987). As a result, the advances in cybersecurity throughout the past several decades have been largely centered on the OSI model. As a means of maintaining organization and historical accuracy, the OSI model will be used as a layout for presenting associative cybersecurity history.

The OSI model should be read from bottom to top. For reference, the physical layer concerns itself with everything on the network with mass. This includes cabling, workstations, hubs, switches, routers, servers, firewalls and any other tangible object (Lammle, Network+ Deluxe Study Guide, 2012). As suggested early in this article, the physical assets were the first and most important piece of early cybersecurity. While the physical security of networking devices can be at risk from such things as flood and fire, the focus here is cybersecurity, the physical risk will be addressed as the protection of sensitive data from physical attack. Physical security is viewed as a barrier that surrounds computing and networking systems that attempts to deter unauthorized physical access to the system itself (Weingart, 1965).

Cyber-physical Security

A protection method rooted in antiquity, human protection refers to the use of an individual or group of individuals acting as a secure barrier for sensitive data (Lammle, Network+ Deluxe Study Guide, 2012). It is quite difficult to attribute an accurate date to the development of this method because it has long been a mainstay of high-importance security. Much like the centurion guards of the Roman expansion, high-value networks and data centers are often patrolled by well-trained security taskforces who defend their sectors up to the point of lethality. ARPANET, having been developed under the watchful eye of the NSA and Department of Defense (DOD), had a large network of cyber-physical security in the United States Armed Forces (Bamford, 2002). This layer of cybersecurity remains a large part of the security methodology practiced at both public and private networking locations.

Locks

Nearly as old as physical guard duty, locks are an essential component of a basic security layout (Lammle, Network+ Deluxe Study Guide, 2012). Much like the binary methods used to protect logical resources, physical locks have evolved with accelerated rapidity (Phillips, 2006). While cybersecurity utilized the mechanical locks that protect the vast majority of homes throughout the world, cyber-locks necessitated continuous advancements as machined locks proved easily accessible by skilled lock pickers (Phillips, 2006). What once was a key-access device soon developed into an electromagnetic lock, accessed with a card-key and personal passcode (Phillips, 2006). By the mid-1990s, biometric access control systems were the new standard for accessing locked server rooms (Phillips, 2006). Unlike a card-key, which could easily be stolen, the new biometric systems used unforgeable means of access control like fingerprints and corneal scans (Phillips, 2006). The implementation of card key systems with biometric functionality was also in large part responsible for the popularity of the layered access control approach. This approach to asset protection began its rise to prominence in the late 1990's and became a feature of standardization that continues into the present (Phillips, 2006).

Closed Circuit Television Surveillance

Common in modern cybersecurity, closed circuit surveillance television (CCTV) found its start in 1949 when the first commercially available camera surveillance system, Vericon, entered the consumer market (Science, 1949). While this is the first mention of a commercially available CCTV system, it is worthy of note that the German government was using CCTV to monitor missile launch and experimentation as early as 1942 (Dornberger, 1954). The earliest CCTV systems allowed for the centralization of security resources allowing multiple locations to be monitored from a single location. The technology became an even more sought after resource after the development of reel-to-reel recording technology in the late 1970s (VinTech, 2011). With the invention of reel-to-reel recording technology, events were no longer limited to live observation, but could also be stored on VHS tapes and examined at a later date (VinTech, 2011). Throughout the last seven decades, video monitoring equipment has evolved into an essential component of data security. Experts in the field have developed standardized practices for installation and setup of CCTV devices, which generally aid in both perimeter and interior cyber-defense tactics (Lammle, Network+ Deluxe Study Guide, 2012).

Cabling

Perhaps overlooked as a substantial development in cybersecurity, the innovation that has occurred in cable development has played a meaningful role in comprehensive cybersecurity. Networks like ARPANET utilized copper coaxial cable that much like telegraph wires, carried short bursts of binary from one node to the other (American Telephone and Telegraph [AT&T], n.d). This medium had been a standard communication tool since being developed by AT&T in 1929 (AT&T, n.d.). The cable coaxial wiring standard was the premier wiring medium all the way up to the Ethernet explosion of the 1970's and continuing into modern networks (Institute of Electrical and Electronics Engineers [IEEE], 2015). The copper wiring Ethernet standards became the basis of the IEEEs 802 standardization, of which multiple standards were written to underline the use of several copper cable types (IEEE, 2015). Cybersecurity however, was not a strong suit for copper cabling. The wiring itself was extremely sensitive to electromagnetic interference (EMI) and could be cut and tapped, allowing tech savvy hackers to intercept network traffic (Lammle, Network+ Deluxe Study Guide, 2012). While shielded twisted pair (STP), a latter development in copper cabling addressed some issues with EMI, it did little to address the physical security threat posed by tapping. By the 1980s, fiber optic cabling had addressed both issues by utilizing a glass core to send light signals in the form of binary communication (AT&T, n.d.). Unlike cable wiring that could be tapped, allowing data streams to be intercepted, cutting fiber optic cable destroyed end-to-end communication, terminating available data streams (Lammle, Network+ Deluxe Study Guide, 2012). Although fiber optic produced both the security and speed desired by the majority of technology professionals, the price of the product has made it a less popular alternative to the CAT5, CAT5e, and CAT6 copper Ethernet standards (Lammle, Network+ Deluxe Study Guide, 2012). As a result, fiber optic cabling is generally reserved for networks carrying highly-sensitive data and corporate-level cyber systems (Lammle, Network+ Deluxe Study Guide, 2012).

DATA LINK SECURITY

A crucial attribute of cybersecurity is the guaranteed delivery of protected data between respective users. While TCP/IP laid the foundations for what would become the routable network at large, it ultimately only provided a high-level overview of necessary functions for Internet operation (Lammle, Network+ Deluxe Study Guide, 2012). In 1964, Paul Baran of the Rand Corporation published a US Air Force study that detailed the earliest proposal of distributed communications; a practice that would later become known as packet switching (Roberts, 1978). The fundamental design proposed by Baran was quickly usurped by both ARPA I between 1962 and 1964, and ARPA II, beginning in 1967 (Roberts, 1978). While the original eleven volume analyses on the matter did provide a basic element of security through integrated encryption, the standard networks of the era functioned more like telegraph components than the multi-connection schemes of modern networks (Roberts, 1978).

At the time that Baran published his work, the basic function of packet exchanged included two adjacent devices, connected by a single cable for communication. When a packet exchange needed to be completed between the two users, the system created enough bandwidth for the transfer only through a single, large block. After the transmission, the bandwidth closed. (Roberts, 1978). While the technique was a fairly reliable means of exchanging information, it lacked both security and a guaranteed delivery to the intended user. Although a great deal of advancement took place between this time and the development of the OSI seven layer model, the standardization of the data link procedures revolutionized the process, adding both security and guaranteed transport (Odom, 2013).

The data link layer of the OSI model is the intermediary between layer one, the physical layer, and layer three, the network layer (Lammle, Network+ Deluxe Study Guide, 2012). Essentially, the data link layer is responsible for determining the physical medium being used to transmit the data, commonly referred to as the media access control (MAC) sublayer, and the logical link control (LLC); which is the network addressing sublayer (Lammle, Network+ Deluxe Study Guide, 2012). As a result of its combined duties, the data link layer is the only piece of the OSI model that works with both the hardware and software components of a network (Lammle, Network+ Deluxe Study Guide, 2012). The data link layer as visible in figure 1 works by breaking large packages into smaller frames and encapsulating them (Lammle, Network+ Deluxe Study Guide, 2012). Each frame is then given three parts, the header, the data to be transferred, and the trailer. The header contains the address of the device that created the frame, as well as the address of the device that will receive it (Lammle, Network+ Deluxe Study Guide, 2012). This allowed for data to be communicated similar to the US Postal mail service delivery. A letter (data packet) is written, placed in an envelope (encapsulation), and then addressed and mailed. The postal service then uses the address to deliver the letter to a specific individual who then opens (decapsulation) and reads the letter (data).

While encapsulation on its own merits a major advantage to cybersecurity, it was not without its pitfalls. Data could still be intercepted between sender and receiver, and, regardless of the original design, delivery was not always a guarantee (Odom, 2013). Furthermore, the earliest forms of data link datagrams often lacked the use of checksum to examine the frame for transmission errors. Accordingly, security development at the data link level included changes to the frame itself, network protocols and network devices.

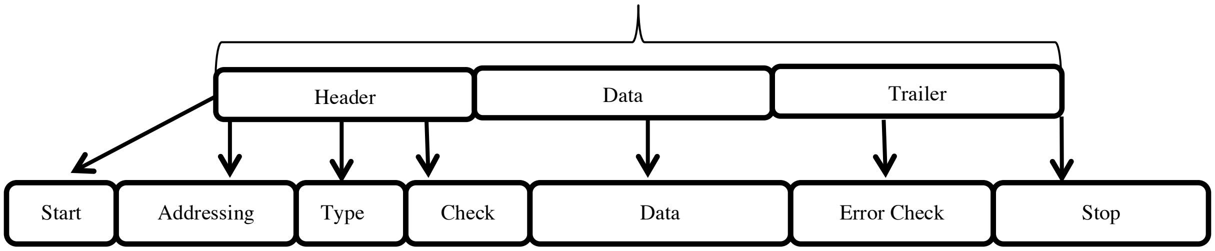

Figure 1. Basic Frame Encapsulation

Switches

Although switches are not necessarily the oldest element of data link layer security, it is arguable that they are the most vital in contributing security to it. The earliest networks exchanged packets via network hubs, which were uncomplicated devices that acted more as repeaters, since they lacked the capacity to examine the data being received (Lammle, CCENT: Cisco Certified Entry Networking Technician Study Guide: ICND1, 2008). In fact, hubs were so basic in their functions that they were considered to be a part of the physical layer their function was to take incoming packets and broadcast them to every node within a network (Lammle, CCENT: Cisco Certified Entry Networking Technician Study Guide: ICND1, 2008). Clearly, if sensitive data needed to be sent from one host to another, the hub was not an efficient means of achieving this task.

In 1990, tech company Kalpana introduced the first Ethernet switch (Technologies, 1995). Switches function much the same way as telephone networks, where one person makes a direct call to a specific destination and only the phone number dialed receives the message (Lammle, CCENT: Cisco Certified Entry Networking Technician Study Guide: ICND1, 2008). Switches, layer two, are in essence the mailmen of a network in that they use the physical address (MAC) of network devices to carry files from one device to another (Lammle, CCENT: Cisco Certified Entry Networking Technician Study Guide: ICND1, 2008). As a result, any machine that is not a specified recipient of the frame will not receive it (Lammle, CCENT: Cisco Certified Entry Networking Technician Study Guide: ICND1, 2008). Further improving the function of these devices is their ability to send and receive messages simultaneously. This was a vast improvement over hubs, which were susceptible to slow-downs since their capacity was limited to sending or receiving, but not both at the same time (Microsoft, n.d.). Regulating packet exchanges to specific users and improving speed meant that information stayed in transit for shorter periods of time, significantly improving both user and network security.

IEEE 802 Standards

The 802 committee was established officially in 1980 in order to develop homogeneous rules for network communications (Kowalenko, 2010). The evolution of the standards through the development of the modern packet switched network has provided many of the fundamental security practices in use today (Kowalenko, 2010). The standard has evolved to include mitigation techniques for many data link layer security threats including MAC spoofing, Content Address Memory table exhaustion attacks, Address Resolution Protocol (ARP) spoofing, and Dynamic Host Configuration Protocol (DHCP) based attacks (Lammle, Network+ Deluxe Study Guide, 2012). The 802 standards introduced the cybersecurity world to technical security essentials, such as limiting the number of allowable MAC addresses to the number of physical hosts in a network, to architectural security solutions such as Spanning Tree Protocol (STP) (Kowalenko, 2010).

Virtual LANs (VLANS)

In 1984, before the modern switch had become a standard networking tool, computer engineer David Sinoskie was developing the foundations for what would become known as virtual local area network (VLAN) (Sincoskie, 2002). Once again, the work was rooted in the study of telecommunications and circuit switching, the basis of modern packet-switched network (Sincoskie, 2002). VLANs function by grouping a number of computers into logical segments and tricking them into believing that they are all operating on a single wire segment, when in fact they are connected to multiple segments concurrently (CISCO, Catalyst 4500 series switch IOS software configuration guide, 2004). VLANs set up broadcast domains that segment and restrict communication to a logical set of computers, allocated to the same VLAN. The benefit of utilizing VLANs is through its capacity to isolate (CISCO, Catalyst 4500 series switch IOS software configuration guide, 2004). VLANs break up larger physical network into smaller, more manageable networks which improves security and performance (CISCO, Catalyst 4500 series switch IOS software configuration guide, 2004). Each VLAN is assigned a single IP address range and then nodes within the VLAN are assigned individual addresses within that range (CISCO, Catalyst 4500 series switch IOS software configuration guide, 2004). The isolation of these services means that even if an attacker gained unauthorized access to the main network, resources would be isolated into multiple harder to reach networks, generally equipped with their own security devices and software (CISCO, Catalyst 4500 series switch IOS software configuration guide, 2004). In other words, a VLAN that operates on the address 10.81.44.X would be limited to communicating solely with devices holding an address between 10.81.44.1 and 10.81.44.254 (CISCO, Catalyst 4500 series switch IOS software configuration guide, 2004).

NETWORK LAYER SECURITY

The network layer is perhaps the most crucial when considering how protection should be implemented. This is because it includes necessary devices and protocols to protect both interior and exterior assets. Unlike the data link layer described above, the network layer encompasses not only the network used to carry packets from device to device within the organizational structure, but also the transfer of packets across the World Wide Web as a whole (Oracle, 1995).

As this is the stratum that interfaces with the extensive global network, it is not surprising that the procedures utilized to provide secure exchanges become more complex. The history of the security measures implemented within this OSI layer spans from Ancient Rome to the modern world of dynamic-automation of security services. Much like the message runners of old, who were responsible for delivering highly-classified materials from one general to the other on opposite battlefields, the modern network infrastructure must provide adequate protection to ensure the lively arrival of the message carrier, while fighting off multiple attacks and enemy combatants.

Networks to the layperson should be considered any situation in which two or more computers are linked to the same source and share information (Technology, 1997). Connecting computers within a network gives users the advantage of sharing resources, communicating in millisecond intervals and combining information as necessary. As this level provides a point of culmination for information and resources, it is an appealing target for criminals. Any network, no matter what infrastructure implemented, is connected to the World Wide Web and is therefore accessible to some degree simply through a public Internet connection. The minute a modem is connected to the service provider, all information contained within the personal network is vulnerable to an external attack (Lammle, Network+ Deluxe Study Guide, 2012).

Network Types

At this point, it is relevant to define the types of networks that are utilized in the sharing of packets and data. Network types are identified by the area that they serve, not necessarily by the number of nodes or devices to which they are attached. The security standards and protocols associated with these different networks do not necessarily change, but the degree to which they are implemented may be impacted by the size of the network in question and the extent to which they deal in highly-sensitive information.

Local Area Networks

A local area network (LAN) is generally a small network that is confined to a limited geographic area such as an office building or even a home (Cole, 2007). As stated in the definition of network types above, it can be populated with any number of devices and users within the network structure, but would not span outside of the suggested building, unless tied to one of the network types listed in the continuation of this article.

Metropolitan Area Networks

A metropolitan area network (MAN) is different from a LAN in that it is generally several buildings that belong to the same organization, whose networking resources are tied one to another forming a network within the same city (Lammle, Network+ Deluxe Study Guide, 2012).

Wide Area Network

A wide area network (WAN) is a series of interconnected devices and resources that encompasses large geographical areas including states and even countries (Lammle, Network+ Deluxe Study Guide, 2012). An organization with services available to its offices in Chicago, New York, London, Paris, and Bali is an example of a WAN.

Encryption

Moving into the actual security practices for the network layer begins with encryption. This is unarguably the oldest method of data protection having served this purpose for the millennia (Institute, History of encryption, 2001). The practice of encryption entails taking information and data and converting it to a series of unreadable characters, so it is intelligible only to the intended recipient(s). The message must be deciphered or decrypted by the intended recipient and therefore, there is usually an exchange of keys or processes between the two sources (Institute, History of encryption, 2001). The first case of documented encryption occurred in 1900b.c. when an Egyptian scribe purposefully used non-standard hieroglyphs to conceal a message (Institute, History of encryption, 2001). The practice was also a highly regarded practice through the rise of Rome. One of the most common forms of encryption, the Caesar Cypher, is attributed (somewhat ambiguously) to notorious Roman ruler, Julius Caesar (Institute, History of encryption, 2001). The cipher as shown in figure 2 was simple in its design, shifting letters by three places in order to conceal the true contents (Institute, History of encryption, 2001).

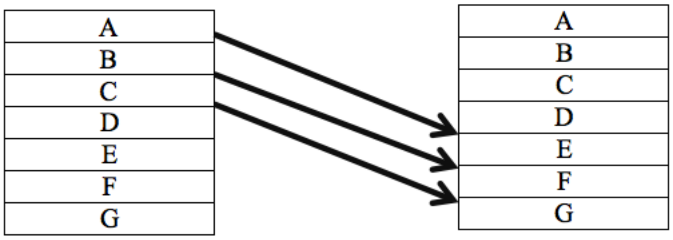

Figure 2. Basic Function of the Caesar Cypher

Modern Encryption

Encryption remained a mainstay of protecting data and top-secret information all the way up through the modern day. It experienced multiple evolutions from the Caesar Cypher, to the renowned enigma machine by Arthur Scherbius; which perplexed allied forces during World War II. This allowed the Axis powers to exchange messages completely cryptic for much of the early part of the conflict (Stripp, 1999). Previously released documents, published under the permission of the NSA, confirms that encryption was commissioned as a standard of data protection as early as the 1940's (Boak, 2007). It could be postulated that the NSA and other security-based organizations have struggled the most with creating an encryption method that could not be easily broken over the past several decades (Boak, 2007). The current model, Advanced Encryption Standard (AES), was recognized as the main encryption practice on October 2, 2000, and is estimated to be an unviable within the next fifteen years (Lammle, 2012). When applied to modern network data-transfers, information can be encrypted both before leaving the network and while in transport. The message can only be decoded by the intended recipient using a decryption key exchanged during the process (Proffit, n.d.).

Access Control Lists

Access control lists (ACL) work much the way the name suggests. An easy way of understanding this mechanism is by comparing it to a real-world situation. For example, an individual goes to a popular inner-city restaurant. Upon entering the establishment, the person is asked by an usher if their name is on the reservation list. If reservations were made and the name was added to the list, then they are taken to a table where they enjoy the services of the establishment. However, if he or she is not on the list, entrance is denied. The same is true of access control lists. ACLs date back to ARPANET, which utilized a database comparison methodology to authenticate users and manage their user-authorizations (Boak, 2007). This process is known as Authentication, Authorization, and Accounting (AAA) (Boak, 2007). In the modern era, the majority of ACL work is handled by the firewall installed in the system, which has simplified the access process.

Firewalls

Firewalls are the guards of the digital kingdom. The firewall made its appearance in the networking world in the late 1980s and it is believed to have originated at the Digital Equipment Corporation, although accounts may differ. What is clear however, is that the first commercially available firewall was issued by DEC SEAL in 1992 (Higgins, 2008). Firewalls, aptly named after the long-standing practice of creating barriers between wildfires and residential areas, allow the administrator of a network to set access rules for their systems (University, n.d.). The most modern and advanced firewalls allow for user-created rules for network control to be added to their list of functions. At their most basic level, firewalls provide network-layer security by restricting the use of both incoming and outgoing port numbers (University, n.d.). A stateful firewall, which is a more modern approach to the firewall ideology, is capable of all of the functions of a normal firewall, but also keeps and manages a historical record of traffic and can therefore make complex decisions about what to allow or deny (University, n.d.).

Intrusion Detection Systems

Intrusion Detections Systems (IDSs) found their start as a result of years of study by the US Air Force, beginning in 1972 (Institute, The History and Evolution of Intrusion Detection, 2001). The concept can be attributed to James Anderson, who in 1980 published a research paper that outlined the use of monitoring and auditing of network traffic as a means of preventing network-security breaches (Institute, The History and Evolution of Intrusion Detection, 2001). The work was brought to fruition between 1984 and 1986 by Dorothy Denning and Peter Neumann, who researched and developed the first IDS prototype utilizing the suggested methods put forth by Anderson (Institute, The History and Evolution of Intrusion Detection, 2001). This prototype developed by Denning and Neumann, the Intrusion Detection Expert System (IDES), would in-time evolve into the IDS platforms in use today (Institute, The History and Evolution of Intrusion Detection, 2001). The modern IDS can be utilized either as a software or hardware product and is either host-based or network-based, depending upon user preference. An IDS is a learning system that familiarizes itself with network baselines and traffic patterns over a short period of time, and then looks for anomalies in these patterns as evidence of network intrusion. Upon detection of an anomaly, it alerts the administrator of possible breaches, prompting action (Institute, The History and Evolution of Intrusion Detection, 2001).

Intrusion Prevention Systems

Intrusion Prevention Systems (IPSs) are similar to IDS in that they monitor baselines and known traffic patterns for incongruities, but the IPS is different in that it does not always require administrative input to handle a network breach (Lammle, Network+ Deluxe Study Guide, 2012). Created in the early 1990s based on the architecture of the IDS, the modern IPS uses signature patterns of incoming data to determine the existence of a threat (Saqueira, 2002). This is a huge benefit over the traditional IDS because instead of relying on baselines for recognition of system breaches, the use of signature-based intrusion detection allows for the system to recognize the type of breach or attack and react accordingly (Saqueira, 2002). Unlike the IDS listed above, the IPS does not need an administrator to intervene. Instead, the IPS has the programmed initiative to deny services to any request that matches its malicious signature inventory (Saqueira, 2002).

Network Address Translation

Network Address Translation (NAT) was conceived by John Mayes and became a standard network addressing practice in 1994 (Tyson, 2001). In a private network, IP addresses are assigned to a pool. In other words, a network administrator uses a range of IP addresses to assign unique values to each device within a network segment. The range of IP address is pulled from a reserved set of private IP addresses known as A, B and C address ranges. There is a Class D and a Class E, but they are reserved specifically for multicast and experimental purposes, respectively. Class A reserves the IP address range 1 -121; class B reserves 128-191; and class C reserves 192-223 (Lammle, Network+ Deluxe Study Guide, 2012). The reserved classes of private addresses are used within the private networks of corporations and organizations throughout the world. It is the job of NAT to intake the private network address at the router and change it to a public, routable IP address (CISCO, Network Address Translation (NAT) FAQ, 2014). In so doing, an entire series of addresses within a network can be reduced to and thereby masked by a single IP address (CISCO, Network Address Translation (NAT) FAQ, 2014). The final security aspect of NAT is in the fact that it memorizes incoming and outgoing IP packets. Any packets that do not meet the recorded information are discarded as “unsolicited” (CISCO, Network Address Translation (NAT) FAQ, 2014).

Antivirus Software

As long as there have been networks, there have been attempts by hackers and crackers to infiltrate them. The number one technique for doing so has long been through the use of viruses. Viruses, much like their name implies, are used to infect a network system and are spread by user interaction. The first virus of record was in 1971, and was dubbed the “Creeper” virus (Bradford, 2011). The Creeper virus infected the ARPANET- which was under the control of the Department of Defense at the time, who in turn deleted the virus using software named “Reaper” (Bradford, 2011). As such, Reaper could easily be considered the very first anti-virus software. Nonetheless, it should be noted that the concept of a virus was not fully defined until the 1980s (Bradford, 2011). Other notable virus battlers of note include Bernd Fix, who successfully utilized his proprietary software to ebb the Vienna Virus in 1987 (Bradford, 2011). The work Bernd did in removing the Vienna Virus is still found in modern anti-virus software, protecting modern computing devices from the very same virus (Bradford, 2011). As far as the development of the first anti-virus software, most experts believe that prestige belongs to Atari, who developed anti-virus software called G-Data anti-virus software (Bradford, 2011). Atari Corp. originally developed the software for their personal computer brand in 1985.

TRANSPORT LAYER

The transport layer of the OSI model busies itself with the actual end-to-end connections that occur between a user-application and user-systems (Stephens, 2011). It is also concerned with reliable data transfer to the upper layers of the model, which will be outlined later in this article (Stephens, 2011). It makes this assured delivery of information using flow control, segmentation, and error control. This guarantee of transmission is directly correlated to the protocols that the transport layer utilizes; transmission control protocol (TCP), and user datagram protocol (UDP). A good explanation for this process is the utilization of your personal banking application. Each time you log into this application to check your balance or pay your bills, it is the transport layer that connects your mobile or personal device to the bank servers, allowing you to interact with their services. Because of the end-to-end connection aspect in conjunction with application-layer interactions, the transport layer utilizes more diverse and complex security techniques that mesh many previously mentioned approaches.

Secure Shell

Secure Shell (SSH) was an answer to the clear text security omissions of both Telnet and r Login, which were remote access protocols of the late 1960s and early 1990s respectively (Target, 2005). As networks began to expand beyond offices and state borders, the need for the ability to administrate these systems remotely became a paramount challenge. More pressing than the need to administrate was the need to administrate securely. SSH was a viable solution to this issue. Developed in 1995 by Finnish inventor Tatu Ylönen SSH relied heavily on encryption to ensure secure end-to-end security (Target, 2005). With SSH, when a user makes a connection, the client and the host exchange keys. If the host recognizes a private key stored within your .ssh folder, it will move to the distribution of a session key that lasts until the connection is terminated, otherwise, if no private key is found, it may ask for a password or utilize another authentication method like Kerberos. Once the connection is made and keys are exchanged to support a session, all communication between the client and host are encrypted using a cypher such as AES (Target, 2005).

Transport Layer Security

Transport Layer Security (TLS) and its earlier incarnation secure socket layer (SSL) are products of chief scientist of Netscape technologies, Dr. Taher Elgamal (Messmer, 2012). Officially recognized as the successor to SSL in 1999, TLS makes use of what has come to be known as the “handshake protocol” (Messmer, 2012). The handshake protocol refers to messages that are passed back and forth between the client computer’s browser and the web or, application server (McKinley, 2003). This is initiated with a secure connection between the two machines, followed by nine more steps: ClientHello, ServerHello, ServerKeyExchange, ServerHelloDone, ClientKeyExchange, ChangeCipherSpec, Finished, ChangeCipherSpec, and Finished. The security in place is used to prevent man in the middle attacks, in which a criminal may try to intercept password and authentication information while data is in transport from client to host (McKinley, 2003). In order for the attacker to decrypt any of the information being exchanged, the masquerader would have to have a copy of the server’s key (McKinley, 2003). The most common use of this security protocol is in the HTTPS framework, utilized by websites that contain sensitive data, such as banking and medical websites.

SESSION, PRESENTATION AND APPLICATION

The previous section identified how the top four layers of the OSI model work heavily in conjunction with one another. The following sections compile the security provisions of the remaining three layers into a single section of the body. While the top layers are collaborative by design, it is still worth taking the time to discuss the services provided by these layers individually.

Session

The first of the three, the session layer is responsible for establishing, maintaining, and terminating connection oriented sessions (Kozierok C. , 2005). It is at this point that we need to change our thinking concerning connections. Previously, we have defined connections as those that exist between two TCP and, port-oriented connections. When we discuss this part of the OSI model, we need to change our thinking to a higher-view of the process, much the way a telephone conversation is carried out between a caller and a receiver. Session-layer protocols handle application to application connection, such as web conferencing, and provide error protection and service guarantees by reestablishing dropped connections. When the user disconnects from the web conference, it is the duty of the session layer to disconnect from the web-service API. In this way it provides a simple layer of security by not allowing random connections to continue in the background (Kozierok C. M., 2005).

Presentation

The presentation layer is not presentation in visual terms. Instead, presentation refers to an action within the OSI model. Instead, the presentation layer is responsible for presenting data to the application layer, one step above (Kozierok C. , The Presentation Layer, 2005). Therefore, the presentation layer must be able to translate multiple forms of data into a standardized format to be interpreted by the associative OSI layers. This includes processes like encryption, covered above; string conversion; data compression; and graphics translation (Kozierok C. , The Presentation Layer, 2005).

Application

The application portion of the OSI model is the final point on the networking tree. This portion of the model is responsible for network applications, as the name suggests (Kozierok C. , The Application Layer, 2005). In the modern tech world, it is easy to mistake application for the programs we run on our personal computing devices. But, instead, applications within the OSI refer to the services utilized by our applications to function on our devices. For example, consider when an individual enters a web address into their browser and hits enter, the protocol used to retrieve and display the page is called Hyper Text Transfer Protocol (HTTP). HTTP is an example of the type of protocol that exists at the application layer (Kozierok C. , The Application Layer, 2005). It is of note to mention that not every application that exists within your library is utilizing the application layer services. If you were to open notepad and begin writing code in the file, it would have absolutely nothing to do with the application layer and would be completely unaware of its existence. However, when you send an email, open a browser, or use a chat program, you are making direct use of application protocols (Kozierok C. , The Application Layer, 2005).

Because the top four layers of the OSI model work together in the vast majority of their functions, a great deal of the security protocols mentioned at the transport layer are also utilized throughout the top three branches of the OSI tree. The use of encryption, password hashing, and key-exchanges are common security modalities at these layers. To avoid tedious repetition, the author leaves it to the reader to review the previous sections for historical reference to these services.

Secure Electronic Transaction

Secure Electronic Transaction (SET), is the result of a combined effort by Visa and MasterCard (Stackpole, 1999). The two credit giants came together in 1996 in cooperation with technology giants like IBM, Microsoft, and RSA to develop protocols that would ensure the security of online credit card transactions (Stackpole, 1999). The protocol is based on X.509 certificate-based security protocols and uses a binding algorithm to secure the exchange of information between parties. The protocol makes use of previously existing application layer protocols to execute this service.

Secure Hyper Text Transfer Protocol

Secure Hyper Text Transfer Protocol (HTTPS) was developed by Enterprise Integration Technologies, which later became known as Veriphone (Stackpole, 1999). Finalized in 1995, it has become the supreme standard for securing web-based interactions. The protocol makes use of the HTTP standards of the application layer, and much like SET, it is rooted in key management and MD5 hash technologies. Unlike SET, however, HTTPS is algorithm independent, giving it the ability to utilize a multitude of options when negotiating security between parties.

CONCLUSION

Cybersecurity has been a pursuit of the technology industry for more than half a decade and much of the technology utilized for cybersecurity is built upon foundations and principles that have been used for decades. Advances in cybersecurity throughout the past several decades have been largely centered on the OSI model, which served as the layout for this overview. The physical assets were the first and most important piece of early cybersecurity, current practices also include cyber-physical security, locks, closed circuit television surveillance and cabling. A crucial attribute of cybersecurity is the guaranteed delivery of protected data between respective users in the data link layer. Data link security, switches, IEEE 802 standards and VLANS are key players in the protection and transmission of data. The network layer is perhaps the most crucial when considering how protection should be implemented. This is because it includes necessary devices and protocols to protect both interior and exterior assets. Those devices and protocols include the network types, encryption practices, access control lists, firewalls, intrusion detection and prevention systems, network address translation and antivirus software. The transport layer handles the end-to-end connections utilizing more diverse and complex security techniques reliant on secure shell, transport layer security and previously mentioned approaches. The remaining layers of the OSI model include the session, presentation and application protocols. The use of encryption, password hashing, and key-exchanges are common security modalities at these layers as well as the use of secure electronic transaction and secure hypertext transfer protocols.

There are currently thousands of security protocols and standards used in network systems around the world. In so being, it would be nearly impossible, short of writing a volumes-based work, of mentioning every standard that has or does exist. This work provides the timeline of cybersecurity implementation and the honorable mentions within the article also represent the most popular and substantial cybersecurity discoveries of the last century. Armed with a solid knowledge of the means by which these theories materialized, evolved, and lead to both new threats and new theories, one can now produce a more accurate picture of where cybersecurity is headed. As mentioned, the key to understanding these theories are the fact that the invention of a single methodology generally leads to further advances, founded in the same principles as the preceding discovery. Due to the very nature of cybersecurity evolution and the rapidity with which cyber threats evolve, it is within all likelihood that many of the standards listed herein will be recommitted to a new standard in a short time span.

REFERENCES

AT&T. (n.d.). *History of Network Transmission*. Retrieved from AT&T: http://www.corp.att.com/history/nethistory/transmission.html

Bamford, J. (2002). *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency.* New York: Double Day.

Blank, A. (2004). *TCP/IP Foundations.* Alameda: Sybex.

Boak, D. G. (2007, December 23). *A History of U.S. Communications Security (Volumes I and II)*. Retrieved from GovernmentAttic: http://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf

Bradford, A. (2011, September 16). *What was the First Antivirus Software?* Retrieved from Anti-virus Software Review: http://anti-virus-software-review.toptenreviews.com/what-was-the-first-antivirus-software.html

Branstad, D. K. (1987). *Networking in Open Systems.* Springer Berlin Heidelberg.

CISCO. (2004). *Catalyst 4500 series switch IOS software configuration guide.* San Jose: CISCO Press. Retrieved from CISCO.com.

CISCO. (2014, November 10). *Network Address Translation (NAT) FAQ*. Retrieved from CISCO: http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Cole, E. (2007, October 26). *Types of Networks*. Retrieved from Sec Lab: Network Security Essentials by Dr. Eric Cole: http://www.sans.edu/research/security-laboratory/article/401-tnetwork-types

Dornberger, W. (1954). *V-2 rocket.* London: Hurst and Blackett.

Higgins, K. (2008, January 15). *Who Invented the Firewall?* Retrieved from Dark Reading: http://www.darkreading.com/who-invented-the-firewall/d/d-id/1129238

IEEE. (2015). *The 40th Anniversary of Ethernet*. Retrieved from IEEE: http://standards.ieee.org/events/ethernet/history.html

Institute, S. (2001). *History of encryption*. Retrieved from SANS Institute InfoSec Reading Room: https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730

Institute, S. (2001). *The History and Evolution of Intrusion Detection*. Retrieved from SANS Institute InfoSec Reading Room: https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344

Kowalenko, K. (2010, May 6). *IEEE 802 Committee Celebrates 30th Anniversary*. Retrieved from IEEE.org: http://theinstitute.ieee.org/benefits/standards/ieee-802-committee-celebrates-30th-anniversary668

Kozierok, C. M. (2005, September 20). *ARP overview standards and history*. Retrieved from The TCP/IP Guide: http://www.tcpipguide.com/free/t_ARPOverviewStandardsandHistory.htm

Lammle, T. (2008). *CCENT: Cisco Certified Entry Networking Technician Study Guide: ICND1.* Indianapolis: Wiley & Sons.

Lammle, T. (2012). *Network+ Deluxe Study Guide* (2nd ed.). Indianappolis: Wiley & Sons.

Microsoft. (n.d.). *How do hubs, switches, routers, and access points differ?* . Retrieved from Microsoft: http://windows.microsoft.com/en-us/windows/hubs-switches-routers-access-points-differ#1TC=windows-7

Mullins, M. (2001, July 2). *Exploring the anatomy of a data packet*. Retrieved from Tech Republic: http://www.techrepublic.com/article/exploring-the-anatomy-of-a-data-packet/

Odom, W. (2013). *Cisco CCENT/CCNA ICND1 100-101.* Indianapolis: Cisco Press.

Oracle. (1995). *Networking basics*. Retrieved from Oracle: https://docs.oracle.com/javase/tutorial/networking/overview/networking.html

Phillips, B. (2006). *The Complete Book of Home, Site and Office Security: Selecting, Installing and Troubleshooting Systems and Devices.* New York: McGraw Hill.

Proffit, B. (n.d.). *Understanding encryption, here's the key*. Retrieved from ReadWrite: http://readwrite.com/2013/09/19/keys-understanding-encryption

Roberts, L. G. (1978, November). *The evolution of packet switching*. Retrieved from IEEE: http://www.packet.cc/files/ev-packet-sw.html

Saqueira, D. (2002). *Intrusion Prevention System: Security's Silver Bullet?* Retrieved from SANS Institute: https://www.sans.org/reading-room/whitepapers/detection/intrusion-prevention-systems-securitys-silver-bullet-366

Science, P. (1949). *Television rides wires.* New York: Popular Science.

Sincoskie, W. (2002). Broadband packet switching: a personal perspective . *IEEE Communicaitons*, 54-66.

Stripp, A. (1999, Novewmber 9). *How the Enigma Works*. Retrieved from Nova: http://www.pbs.org/wgbh/nova/military/how-enigma-works.html

Technologies, L. (1995, August 22). *AT&T makes Ethernet switching as easy as a "Seabreeze"*. Retrieved from Lucent Technologies: http://web.archive.org/web/19970614225541/http://www.lucent.com/press/0895/950822.mea.html

Technology, F. C. (1997). *What is a network?* Retrieved from Florida Center for Instructional Technology: http://fcit.usf.edu/network/chap1/chap1.htm

Tyson, J. (2001, February 2). *How Network Address Translation Works* . Retrieved from How Stuff Works Tech: http://computer.howstuffworks.com/nat1.htm

University, B. (n.d.). *How do firewalls work?* Retrieved from Boston University: http://www.bu.edu/tech/about/security-resources/host-based/intro/

VinTech. (2011, April 20). *Back to Basics: Where Did the Video Security System Come From?* Retrieved from VinTech.com: http://vintechnology.com/2011/04/20/back-to-basics-where-did-the-video-security-system-come-from/

Warner, M. (2012, October). Cybersecurity: A Pre-history. *Intelligence and National Security, 27*(5), 781-799. Retrieved January 6, 2016, from http://www.tandfonline.com/doi/pdf/10.1080/02684527.2012.708530

Weingart, S. H. (1965). Cryptographic Hardware and Embedded Systems - CHES 2000. *Lecture Notes in Computer Science*, 302-317.