

**An Analysis of Security Mechanisms in the OSI Model**

**Karlo Rodriguez  
DTEC 6865**

Merriam Webster's Dictionary defines "security" as "measures taken to guard against espionage or sabotage, crime, attack, or escape". Security can be implemented in a variety of ways. With the ever-growing realm of the cyber world, computer security has undoubtedly grabbed the interest of major corporations and civilians alike. Think about the information stored on your personal computer and the massive quantity of personal information on the computers of major corporations. There is a ton of information that none of us want anyone else having access to (i.e. passwords, social security numbers, bank accounts, etc.) Now imagine having all of that information stolen. What would happen? "Identity Theft" is the illegal use of someone else's personal information in order to obtain money or credit. This could easily be obtained from your computer network if the network is not properly secure. (Merriam-Webster, 2007) Networks can be divided into separate layers using the Open Systems Interconnection (OSI) Basic Reference Model. These layers are, from bottom to top, Physical, Data Link, Network, Transport, Session, Presentation, and Application. A layer is a collection of related functions that provides services to the layer above it and receives service from the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. This paper is about examining the security needed to protect each of the first four layers.

The first layer of the OSI Model is the physical layer. The physical layer defines the Mechanical, Electrical, Procedural and Functional specifications for activating, maintaining and deactivating the physical link between communication network systems. It is the basics of a network. Devices in this layer include hubs, repeaters, cables, and transceivers. (Chandrasekaran, 2002) Basic physical layer troubleshooting revolves around the power source and ensuring the cables are plugged in correctly. To resolve these issues, the network could have an uninterrupted power supply (UPS) installed on its devices so that when the power goes out, the network stays up. The office could also put a lock on the circuit box so no intruders could tamper with it. Interestingly enough, however, the main threat to the physical network is the users of the network themselves. (Surman, 2002)

Social networking is very common when exploiting the physical layer. This is when someone infiltrates your network from the inside. Hackers can gain access to the network by simply walking behind someone into the office as if they are also an employee. One way to prevent this from happening is to issue access cards for employees so they are the only ones with access to the building. You can go one step further and issue access cards that only allow employees access to the areas they work in. Also, users can be given usernames and passwords to identify themselves before they can login to the network. A drawback to this is the risk of losing an access card and/or forgetting one's password. A lot of social networking could be prevented by training the users of the network on what to look for, and how to respond if they notice someone is trying to breach the network. (Gregg, 2007)

Another aspect of social networking is the networking users participate in with their day-to-day activities. When users find themselves with free time at work, many people use that time to browse the internet. Some of this "browsing" is harmless (i.e. checking the weather, news, sports, etc.). However, a task as simple as checking one's personal email could reek havoc on a network. Emails are infamous for containing

viruses, such as the “Melissa Virus.” With the “Melissa Virus,” users would see an attachment in an email from one of their so called “friends” and open it causing the virus to spread throughout the computer. If viruses go undetected, they can continue to spread into the network. Other user errors that can occur are loading random USB flash drives into a computer that contain an autorun-enable causing program that starts before the user even knows what is on the flash drive. (Melissa, 2007)

The next layer of the OSI model is the data link layer. The data link layer is used to transfer data from node to node across a network. The major devices for the data link layer are switches. This is the layer where data packets are prepared for transmission by the physical layer. The data link layer is where MAC addresses and VLANs as well as WAN protocols such as Frame Relay and ATM lie. There are two sublayers in the data link layer. They are the Media Access Control sublayer and the Logical Link sublayer. The MAC Sub-layer is responsible for addressing on the Local Area Network. The MAC Sub-layer is also responsible for determining when nodes on a Local Area Network are allowed to transmit. In Ethernet, this is accomplished using the CSMA/CD protocol. What makes this layer important is that it is used to frame the data for transmission. There are many vulnerabilities at the Data Link Layer that could be discussed, but one of the most important is the Address Resolution Protocol (ARP) process. (Gregg, 2006)

ARP was designed for a more trusting world. It is used to resolve known IP addresses to unknown MAC addresses. When processing packets and passing them down the OSI model, the Data Link Layer is responsible for framing the packets. While the Network Layer will have provided the IP address, the Data Link Layer will need to provide a physical address. That is the job of ARP. It must establish the destination device's physical address when two hosts need to communicate. If the final destination is not local, ARP must still resolve the MAC address of the gateway so that the frame can be properly addressed. Layer two switches are also vulnerable to attacks on their virtual separation of segments known as VLANs. Recent vulnerabilities have been found in Cisco's automatic configuration of VLAN trunks, allowing hosts that can send 802.1Q trunking protocol signaling (an ability that is becoming more and more common in modern operating systems and NIC drivers) to negotiate access to multiple VLANs. Cisco provides configurations to disable this behavior, but the default behavior is to allow automatic VLAN configuration. (Gregg, 2006)

Another way of getting through to the network is by Wardriving. Wardriving, the act of traveling around public areas and randomly accessing 802.11 wireless access points with little to no security settings, is a prime example of a vulnerability with both layer one and two elements. The wireless hardware solution may have an initial goal of ease of deployment and use, but this goal is used as a weakness to exploit the solution for unanticipated purposes on the basis of the solution exceeding its anticipated physical boundaries (the wireless signal extends from the wireless access point's inside location out to the outside public street.) and lacking sufficient use of control at layer two by letting anyone with a signal at layer one to freely connect. A way to combat this is to use encryption methods such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA and WPA2). (Reed, 2003)

Layer three of the OSI Model is called the Network Layer. The network layer defines the network address or IP address, which is different from the MAC address. Some network layer implementations, such as the Internet Protocol (IP), define network

addresses in a way that route selection can be determined systematically by comparing the source network address with the destination network address and applying the subnet mask. Since this layer defines the logical network layout, routers can use this layer to determine how to forward packets. (Teare, 2006)

There are plenty of security vulnerabilities in the network layer. One of these is IP spoofing. This occurs when the intruder sends messages to a host with an IP address (not its own IP address) indicating that the message is coming from a trusted host to gain unauthorized access to the host or other hosts. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host. (IP Spoofing, 2007)

IP spoofing is most frequently used in denial-of-service attacks with the goal being to flood the victim with a lot of traffic. The attacker does not care about receiving responses to his attack packets. Packets with spoofed addresses are suitable for such attacks and these packets are more difficult to filter since each packet appears to come from a different address. Denial of service attacks that use spoofing randomly choose addresses from the entire IP address space. Defenses against denial-of-service attacks that rely on the validity of the source IP address in attack packets might have trouble with spoofed packets. Backscatter, a technique used to observe denial-of-service attack activity in the Internet, relies on the attackers' use of IP spoofing for its effectiveness. (Javvin, 2006)

IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines. For example, it is common on some corporate networks to have internal systems trust each other, so that a user can log in without a username or password provided they are connecting from another machine on the internal network. By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authenticating. (Reed, 2003)

Packet filtering is one defense against IP spoofing attacks. The gateway to a network usually performs ingress filtering, which is blocking of packets from outside the network with a source address inside the network. This prevents an outside attacker from spoofing the address of an internal machine. Ideally, the gateway would also perform egress filtering on outgoing packets, which is blocking of packets from inside the network with a source address that is not inside. This prevents an attacker within the network performing the filtering from launching IP spoofing attacks against external machines. (Javvin, 2006)

Another way a hacker can exploit your network from the network layer is with Routing Information Protocol (RIP) attacks. Routing Information Protocol (RIP) is used to distribute routing information within networks, such as shortest-paths and advertising routes out from the local network. RIP has no built in authentication, and the information provided in a RIP packet is often used without verifying it. An attacker could forge a RIP packet, claiming his host has the fastest path out of the network. All packets sent out from that network would then be routed through that host, where they could be modified or examined. (Javvin, 2006)

Internet Control Message Protocol (ICMP) was designed to act as a messenger for logical errors and diagnostics. It is addressed in detail in RFC 792. Any IP network device has the capability to send, receive, or process ICMP messages. The designers of ICMP never considered the security issues we must deal with today, but they did set some ground rules for ICMP to work efficiently. First was to make sure that ICMP messages wouldn't flood an IP network. ICMP is not given any special priority and is always treated as normal traffic. Second was ICMP messages cannot be sent in response to other ICMP messages. This design mechanism was intended to prevent situations where one error message creates another. Last, ICMP was not designed to be sent in response to multicast or broadcast traffic. (Gregg, 2006)

ICMP is designed so that the header contains a type and code field. Common ICMP types include the following: 0/Echo Reply, 3/Destination Unreachable, 4/Source Quench, 5/Redirect Message, 6/Alternate Host Message, 8/Echo Request, 9/Router Advertisement, 10/Router Solicitation, 11/Time Exceeded. Together, the type and code fields can be used to determine the reason for the ICMP message. For example, a type 3 is a destination unreachable. There are 16 unique codes for type 3 messages. The code identifies the specific reason why the destination is unreachable; this could include a problem with the network (a code 0), a router blocking the packet (a code 13), or even that the application is not running on the destination computer (a code 3). The most common ICMP message type is an 8/0, which is an echo request/reply (ping). There are many network tools built around ICMP. Traceroute is an example of this. Traceroute works by sending numbered IP TTL packets while looking for ICMP TTL exceeded messages returned. With this design, you can see that ICMP can be a very useful network tool. Unfortunately, it is also one of the most used and abused protocols. It's widely used by hackers to verify connectivity before an attack. You cannot attack a system that isn't up and running and ping provides a perfect way to check that a system is alive. This has become so much of a problem that many networks now block incoming initiated pings. (Gregg, 2006)

Another ICMP-related problem is the potential of its use in a denial of Service (DoS) attack. An example of this can be seen in Smurf. Smurf uses ping packets to abuse ICMP. It sends malformed ICMP packets by altering the destination address so that the packet is sent to the broadcast address of a network node. The source address has been altered to be pointed to the victim of the attack. On a large network, many systems will reply to this broadcast ping. The attack results in the victim being flooded with a stream of ping responses so that real access is blocked. A similar type of attack was launched against core DNS servers in 2002. Administrators can prevent their networks from being used to bounce Smurf traffic by adding the following command in their Cisco routers: **no ip directed-broadcast**. ICMP can also be used to aid in port scanning and in OS identification. This is also called fingerprinting. It's a required step of the attack process. An attacker cannot target a system successfully without knowing what its running. For example, the attacker may have an exploit against Windows XP, yet this exploit would be worthless against a Windows 2003 system. Fingerprinting is used to identify the OS. When fingerprinting is attempted, the attacker will use a scanning tool to send a series of normal, unusual and misinformed ICMP queries to the targeted system. The scanning tool then observes the responses and compares them to a database. ICMP was designed for a more trusting world. With all of the functionality ICMP was designed to provide, it

would be nice if it could pass freely in and out of the network. This is not the case, however. If the goal is to make the network more secure, ICMP needs to be blocked and disabled at key network access points as much as possible. The choice will be to drop or reject traffic. From a security perspective, dropping packets gives away less information and makes it harder for an attacker to gather information. Rejecting packets allows services to know that something has failed and time out quickly, yet leaves the network more vulnerable. (Gregg, 2006)

The fourth, and last, layer in the lower section of the OSI model is the Transport layer. The Transport Layer is concerned with the transmission of data streams into the lower layers of the model, taking data streams from above and packaging them for transport, and with the reassembly and passing of incoming data packets back into a coherent stream for the upper layers of the model. Transport protocols may be designed for high reliability and use mechanisms to ensure data arrives complete at its destination. Transport protocols may choose to reduce overhead and simply depend upon the best efforts of the lower layers to deliver the data and the protocols of the upper layers to ensure success to the levels they require. Transport protocols may implement flow control, quality of service, and other data stream controls to meet their transmission needs. (Reed, 2003)

A vulnerability in this layer lies in the use and re-use of ports for multiple functions. This is found quite often in Windows, where differing functions such as file and print sharing, remote administration, LAN messaging, RPC functions, and other applications all use a handful of UDP and TCP ports. This overuse of ports makes restriction of access at layer four by a firewall difficult. If any of the functions are needed, then the firewall ports are opened and most functions that use those ports could flow through unchecked. This overloading limits the effectiveness of network-based controls such as firewalls, and forces reliance on individual host level security controls. These are often not a practical proposition in large enterprise environments, with a large amount of machines operated in many different administrative environments and functional roles. (Reed, 2003)

Conventional firewalls are the most common control at layer four, as well as layer three. Firewall rules should be written to be as strict as possible, regarding transport layer identity. This means that transport layer protocols should be specified individually in rules where possible rather than permitting any communication between two layer three nodes. In terms of TCP/IP communication, this means that rules should be written applying matches for layer four protocols such as UDP/TCP/ICMP as well as subprotocol details such as UDP/TCP port numbers or ICMP types. Modern firewall technology allows for “stateful inspection”, which allows firewalls to inspect the layer four details of a packet and determine the state of a transmission at the transport layer. This allows the firewall to determine if a packet is likely to be in response to an existing flow of data rather than a random packet trying to “sneak by” based on all aspects that govern flow in a given protocol. A more arbitrary packet filter may only check port numbers or simple flags which may be easily determined and set in an arbitrarily assembled packet. (Reed, 2003)

All in all, network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network, the network-accessible resources, and the effectiveness (or lack there of) of

these measures combined together. Implementing network security is paramount due to the sensitive information contained on those networks. Ensuring the privacy of our personal information is critical, and therefore, companies and individuals alike are responsible for taking the necessary measures required to provide that security. Whether you're a new "temp" or corporate executive, everyone plays a role in seeing that security protocols are followed/maintained and that the systems that security is applied to are secure and trustworthy for clientele.

## Bibliography

- Chandrasekaran, Deepak (2002, September, 3). Layer One of OSI Model. from <http://www.boloji.com/computing/networking/n004.htm>
- Gregg, Michael (2006, September, 4). OSI: Securing the stack, Layer 1 -- Physical security threats. from [http://searchnetworking.techtarget.com/tip/0,289483,sid7\\_gci1213436,00.html](http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1213436,00.html)
- Gregg, Michael (2006, October, 2). OSI: Securing the stack, Layer 2 -- Understanding the role of ARP. from [http://searchnetworking.techtarget.com/tip/0,289483,sid7\\_gci1219182,00.html](http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1219182,00.html)
- Gregg, Michael (2006, November, 6). OSI: Securing the Stack, Layer 3 -- The role of ICMP. from [http://searchnetworking.techtarget.com/tip/0,289483,sid7\\_gci1227254,00.html](http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1227254,00.html)
- Gregg, Michael (2007, May, 1). OSI: Securing the Stack, Layer 8 -- Social engineering and security policy. from [http://searchnetworking.techtarget.com/tip/0,289483,sid7\\_gci1253302,00.html](http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1253302,00.html)
- Javvin, (2006). Javvin Technologies. Retrieved November 24, 2007, from Network security layer 3 Web site: <http://2fwww.javvin.com/networksecurity/NetworkSecurityLayer3.html>
- \*Reed, Damon (2003, November, 21). Applying the OSI Seven Layer Network. from [http://www.sans.org/reading\\_room/whitepapers/protocols/1309.php?id=1309&cat=protocols](http://www.sans.org/reading_room/whitepapers/protocols/1309.php?id=1309&cat=protocols)
- \*Surman, Glenn (2002, March, 20). Understanding security using the OSI model.. from [http://www.sans.org/reading\\_room/whitepapers/protocols/377.php](http://www.sans.org/reading_room/whitepapers/protocols/377.php)
- \*Teare, Diane (2006, October, 12). Internetworking Basics. from [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/introint.htm#wp1020694](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#wp1020694)
- (2007, November, 7). Melissa (computer worm). Retrieved November 21, 2007, from Wikipedia Web site: [http://en.wikipedia.org/wiki/Melissa\\_worm](http://en.wikipedia.org/wiki/Melissa_worm)
- (2007, October, 24). IP address spoofing. Retrieved November 21, 2007, from Wikipedia Web site: [http://en.wikipedia.org/wiki/Internet\\_protocol\\_spoofing](http://en.wikipedia.org/wiki/Internet_protocol_spoofing)
- Security. Retrieved November 21, 2007, from Merriam-Webster's Online Dictionary Web site: <http://www.m-w.com/dictionary/security>