REPORT

Tony Z. Tan
Layers of the Stack Research
March 28, 2018

Separation of Layers

As stated in the "Separation of Layers" slide in the Swire presentation, "tech friends comment that there is supposed to be a clear separation of layers of the stack; concern is that this doesn't exist at the non-code layers."

However, the OSI model is also very abstract and theoretical, and in practice, the separation between the technical layers are often not as clear as they initially seem.[1] This is especially true as we move towards the higher layers, such as the session layer, the presentation layer, and the application layer. In fact, in the commonly used Internet protocol suite (TCP/IP model), these layers are merged into one single "application layer."

Cross Layer Attack Examples

In classifying cybersecurity threats, we should note that attacks often do not neatly fit into one specific layer of the OSI model. Here we discuss a few examples.

Layers 1 and 2: Traffic Manipulation on a Local Network

The open nature of wireless networks is a layer 1 weakness, which allows anyone within range to interact with the network without having to bypass physical barriers.

The Address Resolution Protocol (ARP), which links IP (Internet Protocol) addresses to MAC (Media Access Control) addresses on a network, is a layer 2 protocol. The lack of authentication in ARP allows anyone on a network to impersonate another computer on the network and intercept all data sent from and to that computer.

An attacker may combine the open nature of wireless networks with ARP's weakness to intercept and modify data packets sent over a local wireless network, therefore manipulating traffic.

Layers 4 and 7: Vulnerable Application Identification and Exploitation

Different software applications and operating systems rely upon different network ports and protocols to communicate. Consequently, they respond differently to requests received over the

network from other computers. Therefore, an attacker can send specially crafted requests to a computer to determine the operating system and applications that are likely running on the computer. This is known as "fingerprinting" and takes place in Layer 4.

Many operating systems and applications have known weaknesses that attackers can exploit to gain unauthorized remote access. These weaknesses commonly exist in Layer 7.

An attacker can apply "fingerprinting," a Layer 4 technique, to many computers and locate the computers that are running vulnerable software. Then, the attacker can exploit the systems' Layer 7 vulnerabilities to attack and take over computers.

Layers 5 and 6: Acquiring Credentials through Unicode Misrepresentation

Unicode is one of multiple industry standards that prescribe methods for encoding and representing letters and characters using machine code. Because Unicode supports a variety of languages, there are codes representing technically different letters that appear almost identical to each other.

Layer 5 is responsible for authentication, and passwords are commonly used for this purpose. Using the Layer 6 encoding weakness, an attacker can create a malicious website with a web address that is visually identical to that of a legitimate website. If the attacker manages to deceive a legitimate user into entering their password on the malicious website, the attacker can then defeat the authentication by assuming the user's identity.

Layers 3, 6 and 7: Using DNS Cache Poisoning to Attack TLS

Background Information

Internet-connected computers are assigned IP addresses. Entities using the Internet may also register domain names, which serve as human-friendly identifiers that refer to IP addresses. Domain names are powered by the Domain Name System (DNS), which is a Layer 7 service. Computers use DNS servers to translate ("resolve") domain names to one or more IP addresses. To use a DNS server, the computer sends a request to the server with the domain name, and the server responds with an IP address.

To answer the request and resolve a given domain name to an IP address, the DNS server first checks its cache, which stores responses to requests that the server has processed in the past. If the server's cache already has the information requested, and the information is adequately recent, the server responds to the requesting computer with that information.

If the DNS server does not already possess the information necessary to answer the request, it sends a request to the requested domain name's corresponding authoritative name server. A domain name's authoritative name server has ultimate authority over the domain name's DNS records.

The authoritative name server sends a response with the requested information back to the requesting DNS server. The requesting server then responds to the requesting computer with that information and adds the new information to its cache.

The DNS Cache Poisoning Attack

After a DNS server sends a request to an authoritative name server, it waits for and expects a response to its request. In a basic DNS setup, the DNS server, operating in Layer 7, accepts the first response that it receives without extensive verification, so long as the response corresponds to the query, is in a valid format, and purports to come from the authoritative name server.

In one variation of the DNS Cache Poisoning attack, the attacker first sends a request to the DNS server asking for the IP address of a target domain name. Then, the attacker begins to continuously send false ("spoofed") responses to the DNS server. Using a weakness in Layer 3, the attacker impersonates the target domain name's authoritative name server by modifying the response metadata and falsifying origin information. This false response may, for example, resolve a legitimate target domain name to a malicious IP address that is controlled by the attacker.

If the DNS server did not already have the target domain name's information in its cache at the outset of the attack, it would send a request to the domain name's authoritative name server. If the DNS server receives and accepts the spoofed response from the attacker, it would add the false DNS record supplied by the attacker to its cache.

With the false DNS record now in the DNS server's cache, all computers that rely upon this server to resolve domain names will also be provided with the incorrect record when they request the IP address of the target domain name. The attacker has successfully executed a DNS cache poisoning attack, redirecting data intended for a legitimate computer to one controlled by the attacker.

Obtaining Unauthorized Certificates to Attack TLS

Transport Layer Security (TLS) is a Layer 6 protocol that protects the security of user connections to websites. TLS and other commonly used security protocols depend on Digital Certificates for important security properties and assurances. Digital Certificates for website

encryption (TLS Certificates) are issued by specialized organizations (Certificate Authorities) after the requester's administrative control of the website is verified.

One method commonly used by Certificate Authorities (CA) to verify administrative control is to send a verification code via email to the website administrator's email address, such as "admin@example.com."

If an attacker successfully launches a DNS Cache Poisoning attack against the CA's DNS server and causes the CA's system to send the verification code to the attacker instead of the legitimate administrator of a target website, the attacker may be issued a cryptographically valid TLS Certificate for the target website.

Armed with the mis-issued but cryptographically valid TLS certificate for the target website, the attacker would be able to compromise the security of "secure connections" to the website, including by intercepting and modifying data transmitted to the website without affecting security indicators or triggering security warnings.

Works Cited

[1]R. Maupin, "Answer: In which OSI/TCP-IP model layers do BGP, RIP protocols belong?", *Network Engineering Stack Exchange*, 2015. [Online]. Available: https://networkengineering.stackexchange.com/questions/24255/in-which-osi-tcp-ip-model-layers-do-bgp-rip-protocols-belong. [Accessed: 14- Feb- 2018].

[2]G. Surman, "Understanding Security Using the OSI Model", *SANS Institute InfoSec Reading Room*, 2002. [Online]. Available: https://www.sans.org/reading-room/whitepapers/protocols/understanding-security-osi-model-377. [Accessed: 28- Feb- 2018].

[3]P. Wolff, "Evi Nemeth's 9-Layer OSI Model", *Flickr*, 2006. [Online]. Available: https://www.flickr.com/photos/philwolff/96987427. [Accessed: 28- Mar- 2018].

[4]"ISC 9-Layer OSI Model Cotton T-Shirt", *Internet Systems Consortium*, 2015. [Online]. Available: https://www.isc.org/product/isc-9-layer-osi-model-cotton-t-shirt/. [Accessed: 28- Mar- 2018].

[5]R. Miller, "The OSI Model: An Overview", *Sans.org*, 2001. [Online]. Available: https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543. [Accessed: 28- Mar- 2018].

[6]K. Shaw, "The OSI model explained: How to understand (and remember) the 7 layer network model", *Network World*, 2017. [Online]. Available: https://www.networkworld.com/article/3239677/lan-wan/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html. [Accessed: 28- Mar- 2018].

[7]A. Russell, "OSI: The Internet That Wasn't", *IEEE Spectrum: Technology, Engineering, and Science News*, 2013. [Online]. Available: https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt. [Accessed: 28- Mar- 2018].

[8]S. Crutchley, "Information Security: Addressing the Human Factor", *iTnews*, 2004. [Online]. Available: https://www.itnews.com.au/feature/information-security-addressing-the-human-factor-61687. [Accessed: 28- Feb- 2018].

[9]"Layer 8", *English Wikipedia*, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Layer_8. [Accessed: 28- Feb- 2018].

[10]L. Kachold, "Layer 8 Linux Security: OPSEC for Linux Common Users, Developers and Systems Administrators", *Linux Gazette via Internet Archive*, 2009. [Online]. Available: https://web.archive.org/web/20090705093433/http://www.linuxgazette.net/164/kachold.html. [Accessed: 28- Feb- 2018].

[11]"Layer 8 Performance Issues - Apposite Tech", *Apposite Tech*, 2017. [Online]. Available: http://www.apposite-tech.com/blog/osi/layer-8/. [Accessed: 28- Feb- 2018].

[12]"The Layer 8 Initiative", *NC State University via Internet Archive*, 2005. [Online]. Available: https://web.archive.org/web/20070210031959/http://www.ncsu.edu/it/cmptplans/layer8/. [Accessed: 28- Feb- 2018].

[13]D. Reed, "Applying the OSI Seven Layer Network Model To Information Security", *SANS Institute InfoSec Reading Room*, 2004. [Online]. Available: https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309. [Accessed: 28- Feb- 2018].

[14]R. McOrmond, "Layer 8 (Financial) and layer 9 (Political) of the OSI protocol stack", *Flora.ca*, 2004. [Online]. Available: http://www.flora.ca/osw2004/osw2004.pdf. [Accessed: 28- Feb- 2018].

[15]J. Gogan, "The OSI Model", *The University of North Carolina at Chapel Hill*, 2005. [Online]. Available: https://www.unc.edu/~gogan/osi.html, https://www.unc.edu/~gogan/osireal.html. [Accessed: 28- Feb- 2018].

[16]S. Curry, "Engineering Security Solutions at Layer 8 and Above", *The RSA Blog and Podcast via Internet Archive*, 2010. [Online]. Available:

https://web.archive.org/web/20120708004413/http://blogs.rsa.com/curry/engineering-security-solutions-at-layer-8-and-above. [Accessed: 28- Feb- 2018].