**Topic:** Security Architecture and Design

**Question:**

What happens when we place the authentication system in our demilitarized zone (DMZ)—that is, in the layer closest to the Internet? What do we have to do to protect the authentication system? Does this placement facilitate authentication in some way? How about if we move the authentication system to a tier behind the DMZ, thus, a more trusted zone? What are the implications of doing so for authentication performance? For security?

**Instructions:**

* Need 3 Responses for other student posts
* Minimum 150 words for each response (use uploaded document to see other student posts)
* No plagiarism please

**Initial Post 1:**

One of the most useful tools in firewall engineering today is the DMZ, or Demilitarized Zone, a network where all publicly accessible services are placed so they can be more closely watched and, also, isolated from one's the internal network (Stuart, 2015). DMZs, bastion servers and Linux make a particularly good combination.

What happens when we place the authentication system in our demilitarized zone (DMZ)  is we allow access to resources from untrusted networks while keeping the private network secured. Resources commonly placed in the DMZ include Web servers, Mail servers, FTP servers, and VoIP servers.

As systems that are most vulnerable to attack are those that provide services to users outside of the local area network, such as e-mail, Web and Domain Name System (DNS) servers, they are ‘quarantined’ inside a DMZ, from where they have limited access to the private network. Hosts in the DMZ can communicate with both the internal and external networks, but communications with internal network hosts are tightly restricted.

This placement facilitates authentication in some way. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ (Scott, 2011). For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

**Initial Post 2:**

In computer security, a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an internal network and an external network (Michael ,2003). The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network -- hosts in the DMZ may not connect to the internal network.

Unlike the geopolitical DMZ, a DMZ network is not a no-man's land that belongs to nobody. When you create a DMZ for the organization, it belongs to you and is under your control. However, it is an isolated network that's separate from your corporate LAN (the "internal" network). The DMZ uses IP addresses belonging to a different network ID.

To protect the authentication system, each and every user should have their own, unique, set of credentials that are known only to them (Scott, 2011). There should never be a master admin account that is used by several SysAdmins, and every time an admin must unlock or reset an end user’s account, they need to set a temp password that must be changed at next logon. This can be harder to manage, but I recommend not even using the same initial password for new users, as that is something a lot of people are going to know and could be used with a new hire’s account before the day they start.

**Initial Post 3:**

In computer networks, a DMZ (demilitarized zone), also sometimes known as a perimeter network or a screened subnetwork, is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks -- usually the internet. External-facing servers, resources and services are located in the DMZ (Scott, 2001). Therefore, they are accessible from the internet, but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data via the internet.

As a DMZ splits a network, security controls can be tuned specifically for each segment. For example, a network intrusion detection and prevention system located in a DMZ and providing web services could be configured to block all traffic except HTTPS requests to TCP port 443.

The more secure approach to creating a DMZ network is a dual-firewall configuration, in which two firewalls are deployed with the DMZ network positioned between them. The first firewall -- also called the perimeter firewall -- is configured to allow external traffic destined to the DMZ only. The second, or internal, firewall only allows traffic from the DMZ to the internal network (Maiwald, 2003).. This is considered more secure because two devices would need to be compromised before an attacker could access the internal LAN.

The accessible buffer the DMZ provides prevents an attacker from being able to scope out potential targets within the network (Cobb, 2018). It makes internal reconnaissance more difficult because even if a system within the DMZ is compromised, the private network is still protected by the internal firewall separating it from the DMZ.