Defense Models

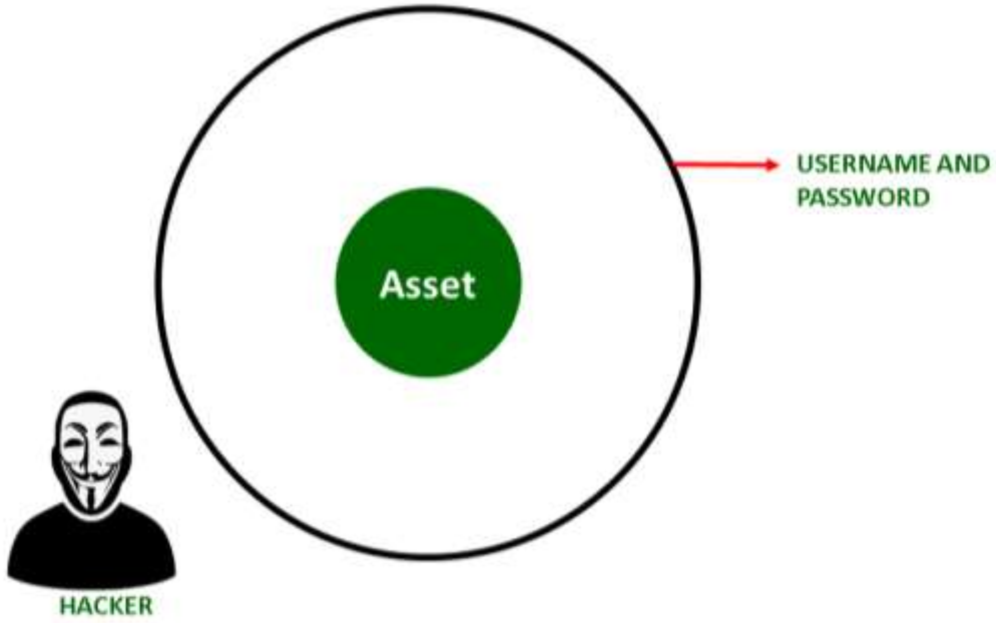
In order to preserve the confidentiality, integrity, availability, and authenticity of electronic and physical assets such as the data on a network, it is important to build a defensive perimeter around those assets and trust everyone who has access inside and use many different types and levels of security controls in a layered defense-in-depth approach.

The two most common approaches to security are Lollipop Model and Onion Model.

The Lollipop Model

The most common form of defense, known as perimeter security, involves building a virtual (or physical) wall around objects of value. Perimeter security is like a lollipop with a hard, crunchy shell on the outside and a soft, chewy center on the inside.

Consider the example of a house—it has walls, doors, and windows to protect what's inside (a perimeter). But it does not make it impenetrable. Because a determined attacker can find a way in—either by breaking through the perimeter, or exploiting some weakness in it, or convincing someone inside to let them in. By comparison, in network security, a firewall is like the house—it is a perimeter that can't keep out all attackers. Yet the firewall is the most common choice for controlling outside access to the internal network, creating a virtual perimeter around the internal network (which is usually left wide open). This often creates a false sense of security, because attackers can break through, exploit vulnerabilities, or compromise the network from the inside.



One of the limitations of perimeter security is that once an attacker breaches the perimeter defense, the valuables inside are completely exposed. As with a lollipop, once the hard, crunchy exterior is cracked, the soft, chewy center is exposed. That’s why this is not the best model of defense.

Another limitation of the lollipop model is that it does not provide different levels of security. In a house, for example, there may be jewels, stereo equipment, and cash. These are all provided the same level of protection by the outside walls, but they often require different levels of protection. On a computer network, a firewall is likewise limited in its abilities, and it shouldn’t be expected to be the only line of defense against intrusion.

A lollipop defense is not enough to provide sufficient protection. Yet many organizations do not understand firewalls in this way. Firewalls are an important part of a comprehensive network security strategy, but they are not sufficient alone. Today, networks both send information to and receive information from the Internet, and the rules for doing so are complex. Firewalls are still useful for shielding networks from each other, but they are often not sufficient to provide proper access controls, especially when internetwork communication and network resource sharing are complicated. Firewalls are an important part of a complete network security strategy, but they are not the only part. A layered approach is best.

The Onion Model

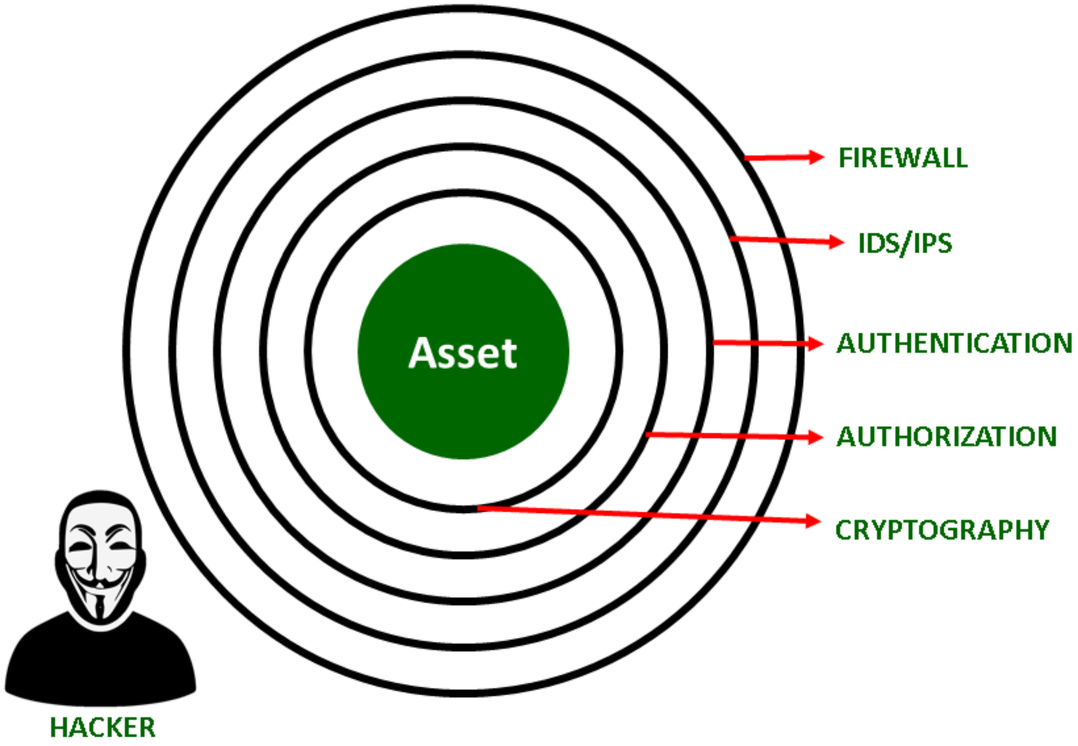
A better approach is the onion model of security. It is a *layered strategy*, often referred to as *defense in depth*. This model addresses the contingency of a perimeter security breach occurring. It includes the strong wall of the lollipop but goes beyond the idea of a simple barrier. A layered security architecture, like an onion, must be peeled away by the attacker, layer by layer, with plenty of crying.

Consider what happens when an invader picks the front door lock or breaks a window to gain entry to a house. The homeowner may hide cash in a drawer and may store valuable jewels in a safe. These protective mechanisms address the contingency that the perimeter security fails. They also address the prospect of an inside job. The same principles apply to network security. It needs to be taken into account what happens when an attacker gets past the firewall or, what happens when a trusted insider, like an employee or a contractor, abuses their privileges. The onion model addresses these contingencies.

A firewall alone provides only one layer of protection against threats originating from the Internet, and it does not address internal security needs. With only one layer of protection, which is common on networks connected to the Internet, all a determined individual has to do is successfully attack that one system to gain full access to everything on the network. A layered security architecture provides multiple levels of protection against internal and external threats.

The more layers of controls that exist, the better the protection against a failure of any one of those layers.

Consider a system that allows full access to an account that only uses username/password authentication, without any other security controls. That system uses only one layer of security, and it is strictly an authentication control. Anyone who obtains the username and password, or hijacks an account that's already logged in, can gain full access to the system. Since there are no other layers that must be bypassed, the system would be completely compromised. If such a system had further layers of security controls that needed to be passed after the username and password authentication, compromising the system would be correspondingly more difficult.



The layered security approach can be applied at any level where security controls are placed, not only to increase the amount of work required for an attacker to break down the defenses, but also to reduce the risk of unintended failure of any single technology.