Providing WLAN Security with RBAC & Policy

Scott Lester

Over the years, customers have become increasingly aware of the need for data security within their organization. In many cases, institutions such as healthcare and financial organizations have been required by government and industry regulations such as HIPAA, PCI, and Sarbanes-Oxley to instantiate policies to help prevent data leakage from their networks that include wireless devices. In a recent project, I was tasked with helping a healthcare organization implement a NAC product that would help provide role-based access control to wireless devices within their network. As part of this project, it was also necessary to help the organization craft a functional security policy that would help define the workflows and device policies within the RBAC system.

I began the process of building the functional policy by determining the different device types that would be present in the WLAN and what level of network access each of these device types would require. The device types were then categorized into six groups that would form the basis of our RBAC policies: VOIP, Medical, Guest, Employee, Vendor, Physician. Next, I worked with the customer to determine the type of wireless encryption best suited for each device type and how those devices would connect to the WLAN. I needed to combine some of these device categories since only four SSIDs would be broadcast in the WLAN to meet the design criteria set by the customer. I determined that the physicians, vendors, and employee categories could be combined as each of these categories would utilize 802.1X/EAP-TLS authentication with WPA2/AES encryption. The 802.1X process relies on information from the AAA framework to provide user authentication, authorization, and accounting. Since EAP-TLS requires mutual authentication to validate both the supplicant and authentication server, this method of authentication provided a higher level of security (over PSK) that was required because of the sensitivity of data available to these devices. Also, the ability to manipulate network access based on RADIUS attributes returned during the 802.1X process would be needed as each device category would have different network permissions. For medical devices, the encryption type of WPA2/AES PSK was selected based upon device limitations concerning the lack of support for 802.1X/EAP-TLS authentication. VOIP devices would use WPA2/AES PSK encryption due to the length of time for authentication/association being much faster than that required to complete 802.1X/EAP authentication. The 802.1X authentication process relies on multiple exchanges between the VOIP device (supplicant) and NAC appliance (authentication server) to authenticate the user and provide the seeding material needed for the temporal key creation during the 4-way handshake. With the amount of time required for this exchange and 4-way handshake exceeding real-time voice packet tolerances of 150ms, roaming speed and voice quality can be greatly diminished and/or broken. With WPA2/AES PSK, the exchanges between the supplicant and authentication server are eliminated, with the PSK providing the seeding material needed for the master session key (and subsequent temporal key generation) during the 4-way handshake. The reduction in authentication/association time provided by WPA2/AES PSK was needed to reduce roaming times and provide ensure voice quality within the WLAN. Finally, as guest users on the network would only require basic internet access, they would be placed on an open network with no data encryption.

Once the SSID classifications and authentication/encryption methods were completed, I began crafting the service workflows within the NAC system that would handle enforcement of the network security policy. The workflow for the guest network would enforce the usage of a captive portal page for guest registration, that would also limit the number of guest devices on the network. The captive portal page would also provide access to the device onboarding application used to provision devices connecting to the 802.1X network, that were previously unknown to the NAC. For VOIP and medical devices, the workflow would need to include a way to ensure only allowed devices were connecting to these networks and this was accomplished by using a method known as device fingerprinting. Fingerprinting is a method used within the NAC to identify devices based on methods such as DHCP and HTTP snooping that takes information from the DHCP process and/or HTTP communication to create a fingerprint that is common to each unique device type. The last workflow to create would involve the highest level of difficulty as multiple levels of authorization would be required within each device category of employee, physician, and vendors. Within this service workflow I created rules that utilized authorization information returned during the 802.1X process to determine which device category the user belonged. Next, I utilized information from the device fingerprinting process to classify the device type as the organizations' security policy prohibited the use of personal devices in the same VLAN as hospital owned devices. The NAC would then use an enforcement policy within the workflow that evaluated current device accounting information and compared that to information returned from the 802.1X authorization information, issuing a RADIUS CoA that would cause the device to move to the correct network if required. The CoA was used instead of waiting until the client logged out and back in to the network, to enforce the correct level of network access immediately. As a last step, each of these workflows (with the exception of the guest network) contained a rule that denied access to the network.

By utilizing the processes involved with each of the various WLAN security and encryption methods available within the 802.11 standard, I was able to help the customer increase the level of security within their network.