STRIDE and DREAD Assessment

Note: I used the original STRIDE and DREAD article written by Meier et al. (2003) as a point of reference.

Brute Force

Since the goal of a brute force attack is to obtain a password and thereby impersonate a valid user, it can be said that brute force attacks fall within the spoofing category of the STRIDE model. A relevant suggested coutnermeasure is to use strong passwords. In my forum post, I also suggested the use of strong passwords but discussed how this can be done, namely by ensuring that passwords have a high entropy. In the context of a password, entropy can be explained as how unpredictable a password is (GeneratePasswords, n.d.), which can be thought of as the potential combinations that a given set of password rules would have. As an example, a password that is numeric only would have an extremely low entropy, whereas a recommended password (containing upper/lower case letters, numbers, and symbols) would have a much higher entropy, and therefore be practically impossible to crack using a brute force attack.

According to the DREAD model, these would be the points for a brute force attack:

D = 3 points, because the attacker could relay fraudulent data from the mannequin and manipulate the data shown. R = 3 points, because there is no situational component to this kind of attack. E = 1 point, because the attack requires that the victim uses WPS for router authentication. A = 3 points, because the device requires WiFi to function and thus all users are affected. D = 3 points, because published information is available with an exact series of steps provided, and it is easy to identify if a router uses WPS.

DoS

Denial-of-service attacks (DoS) are defined within the STRIDE framework. Meier et al. (2003) recommend the usage of resource throttling along with input validation, while in my forum post, I recommended infrastructural changes.

In the STRIDE model, DoS attacks are assigned their own category. The following section outlines the DREAD analysis for the DoS attack. The DREAD scale from the given article is reused, but the "damage potential" metric is redefined as the initally given measurements are not usable in the case of a DoS. The following scale is used, based on my interpretation of the situation: 1 = the attacker can cause periodic outages on a single device, 2 = on a single device, the attacker can trigger an indefinite outage, 3 = the attacker can cause indefinite outages across multiple devices and networks. The DREAD scores are therefore as follows:

D = 2 points, because this attack could cause an indefinite outage on a device, but the attacker would need to be near the device, meaning that it is difficult to attack multiple devices simultaneously. R = 3 points, because the steps for initiating this attack have no situational component. E = 3 points, because no programming knowledge is necessary- all that is required are some command-line tools and a small amount of knowledge on how command-line interfaces work. A = 3 points, because the device requires WiFi for communication and therefore all users would be affected. D = 3 points, because there is published documentation available which describes the exact software necessary and the steps that must be taken to cause a DoS.

Analysis

The total DREAD score for the brute force attack is 13 points, while the total score for the DoS attack is 14 points. The brute-force attack is much less exploitable than the DoS attack (since its exploitability score is

lower), while the DoS attack has a lower damage potential. After accounting for all other factors, however, it can be said that the DoS attack poses a greater threat. This conclusion holds under the assumption that routers under attack all use WPS.

References

Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. & Murukan, A. (2003) Chapter 3 – Threat Modeling. Available from: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN [Accessed 21 November 2021].