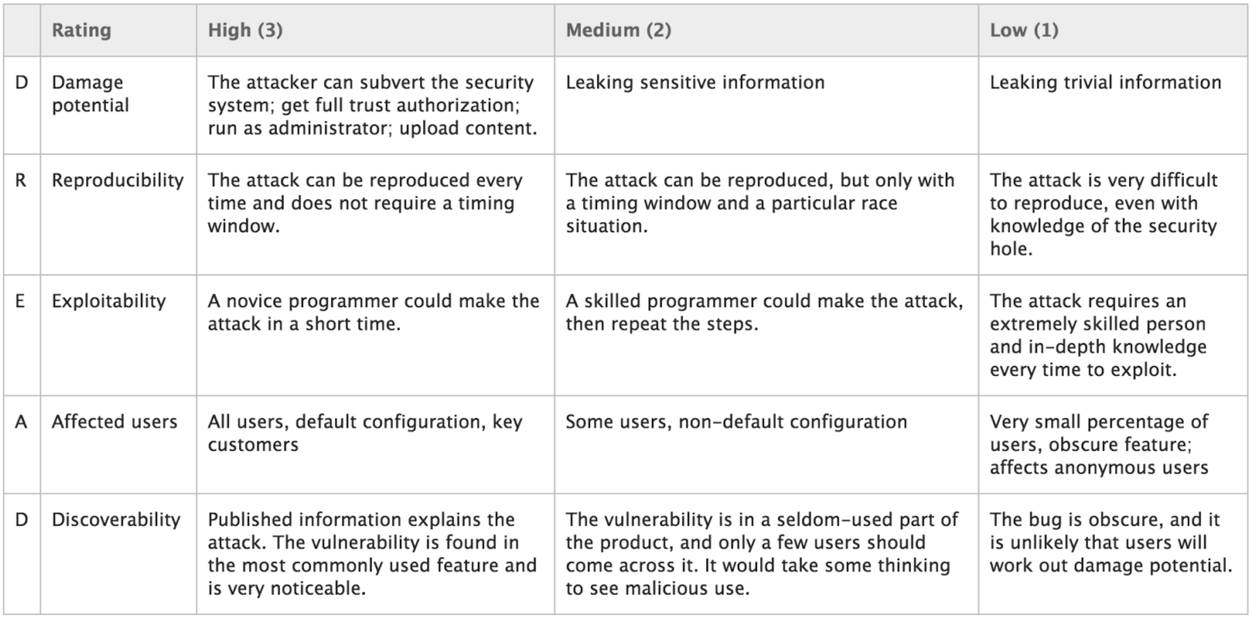
Risk Rating Metric -- Variant of Microsoft DREAD

At the beginning, I considered to refer DREAD risk rating methods from Microsoft. The original DREAD consists of 5 parts,

- Damage potential(D)
- Reproducibility(R)
- Exploitability(E)
- Affected users(A)
- Discoverability(D)

with details shown in the form below:



	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in–depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non–default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom–used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

DREAD defines each parameter with different level(generally High/Medium/Low) and assigns corresponding score ranges, then calculates the sum of all five parameters as the final result. The final score will be mapped into different ranges which refer to different level of severity.

DREAD is a very simple and classical method to produce evaluation for security risks. However, it was designed to be used for assessment of high-level security areas, especially for applications' security. It is even barely used for threat modeling in network layer, so does the second layer which is the core research environment of this project. Thus, lots of definitions, such as the five parameters and detailed description for each of them, can not be referred directly. Changes need to be made so that it can be more fitable in public wireless network scenarios.

Firstly, I considered to alter the definitions for some parameters, mainly for following two parameters:

- Damage potential: How great is the damage if the vulnerability is exploited?
  - Low: Leaking trivial information, e.g. existence, MAC address, general information of user's devices, request packets header/content(no sensitive information exposed)
  - Medium: Leaking sensitive information(in plaintext), fake authentication and association.
  - High: Attacker can get full trust authorization, run as administrator, fully control all communications, access to user's local directory/system privilege, etc.
- Affected Users
  - Low: Targeted at random user
  - Medium: Targeted at certain user
  - High: Targeted at AP, which will affect all users connected to it.

Then, I realized that some additional parameters need to be added into the original metrics, since they need much more concentration when talking about public wireless hotspots than generic application security:

- Additional One: Time Consuming (Since most of public Wi-Fi users connect to AP temporarily, if an attack can be successful in theory but need to take very long time to exploit, it will have less risk for normal users).
  - Very Low: > 1 hr
  - Low: 30 mins - 1 hr
  - Medium: 15 mins - 30 mins
  - High: 5 mins - 15 mins
  - Very High: < 5 mins

- Additional Two: Potential usage for further attack, further attack's severity and contribution to further attacks.
  - Very Low: Hard and less severe
  - Low: Hard and severe
  - Medium: Not hard and not so severe
  - High: Easy and not that severe
  - Very High: Easy and very severe

Furthermore, I thought it is not that reasonable to use the sum of all parameters as the final result, Since among the current 7 parameters, 3 are for damage, 4 are for possibility, also for some special reason with wireless network, there are many situations that a threat always has very high possibility to be exploited but it's effects could be limited or just be as a trivial step for other threats. It's the tight relationship between all threats that makes DREAD not that practical in this occasion. So I consider to combine the extensioned DREAD parameters with classical formula "Risk = Damage * Possibility", and give this final rating method:

Damage Potential	Affected Users	Further Attack	Exploitability	Reproducibility	Discoverability	Time Consuming

Risk = (D+A+F)(E+R+D+T)*

And I assigned various weights for different parameters. In sum, total score for damage counts the same as total score for possibility. All parameters of possibility share same weights. Damage Potential and Further attack counts a little more than Affected Users, since range of affection in this situation is not that important due to the radio wave feature of wireless network.

Calculation for total score:
(3.5+3+3.5) * (2.5+2.5+2.5+2.5) = 100

Score Distribution of Severity Levels: S>A>B>C>D

0-19	D
20-39	C
40-59	B
60-79	A
80-100	S