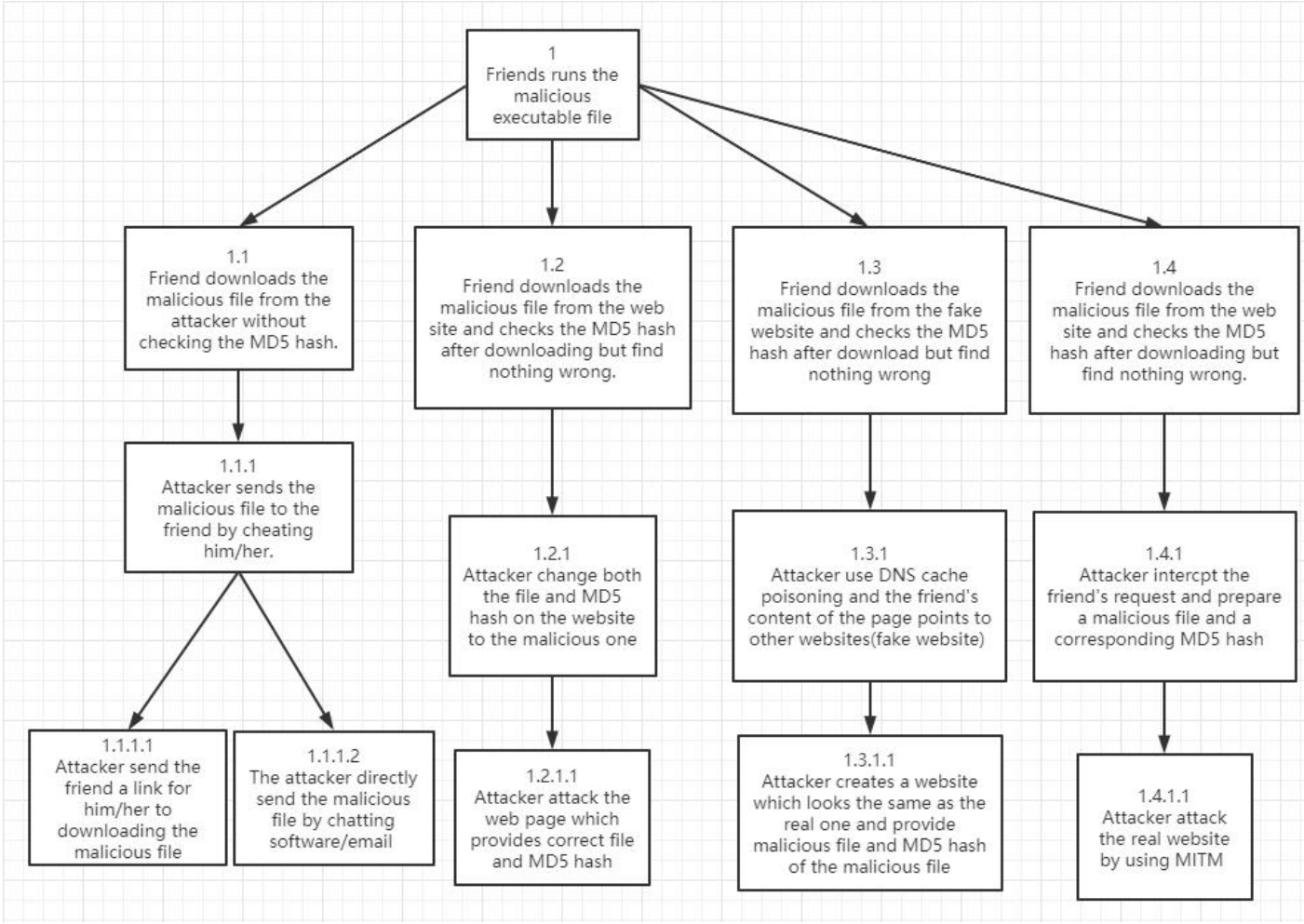
1. Attack Tree




2. Discussion

The path 1 -> 1.3 -> 1.3.1 -> 1.3.1.1 would be most likely to succeed

2.1 Why the other path is not likely to succeed.

First of all, it is very difficult to gain the trust of friends. Generally speaking, they are more likely to download files from the original website rather than accept a file from other guys. Besides, we cannot prevent them from doing hash value verification. So we need a way to change the file without the friend knowing it.

Second, It is not easy to attack the original website. The website master is very likely to find out that the website has been attacked and take defensive measures in time, or directly inform students to suspend downloading files.

2.2 Why this path is likely to be succeed.

There is a time lag between when the computer sends a "domain name query" request to the domain name server and the domain name server sends the response to the computer. If an attacker can forge a wrong DNS response and send it to the computer before the DNS response from the DNS server reaches the computer. So the computer receives the wrong message and gets a wrong IP address. Thus, by using DNS cache poisoning, we can easily redirect the friend to the fake website created by the attacker without knowing it. Even if the friend doing hash value verification, he/she will not find that the file is a wrong one.

2.3 How this attack path could be mitigated.

(1) Use a variety of SSH encryption agents, remote DNS resolution in the encryption agent, or use

VPN to access the Internet.
(2) When modifying the hosts file, the privilege priority of hosts file in the operating system is higher than that of DNS server. When the operating system accesses a domain name, it will first detect the hosts file, and then query the DNS server. The contaminated DNS address can be added to hosts to solve DNS pollution and DNS hijacking.
(3) Through some software programming processing, we can directly ignore the packet with false IP address, and directly solve the problem of DNS pollution.