Yining Wang

504983099

CS35L Assignment 10

2018/12/6

New security flaw discovered in Wi-Fi routers

A research team from UC Riverside found a security flaw of modern computers caused by the nature of TCP protocol and Wi-Fi routers. Sadly, the nature of this flaw makes sure that it cannot be fixed easily.

Some background knowledge is essential to learn what is going on in this flaw. According to UC Riverside New.com, “TCP breaks information into manageable chunks that can be transmitted between computers over the internet. Each chunk, known as a “packet,” receives a number within a sequence unique to that particular communication that ensures it is delivered correctly. The first number of the initial sequence is randomly chosen, but the next numbers will increase predictably, so the receiving computer can arrange them properly if they arrive out of order.”, and “Wireless routers can only transmit data in one direction at a time because they communicate with devices in their network on a single channel. Like walkie-talkies, if both parties send information at the same time, there will be interference. This is known as a half-duplex transmission, a characteristic of all wireless routers.”

The fundament of this flaw is that because of the half-duplex nature of Wi-Fi routers, when some packages are sent from a server to a client through TCP protocol, the time interval between the server receiving the package and replying whether the

package is “good” or not, or whether the number attached to that package is the next number of the number sequence of that specific transmission, is somehow relevant to if the number the server give is close enough to the correct number.

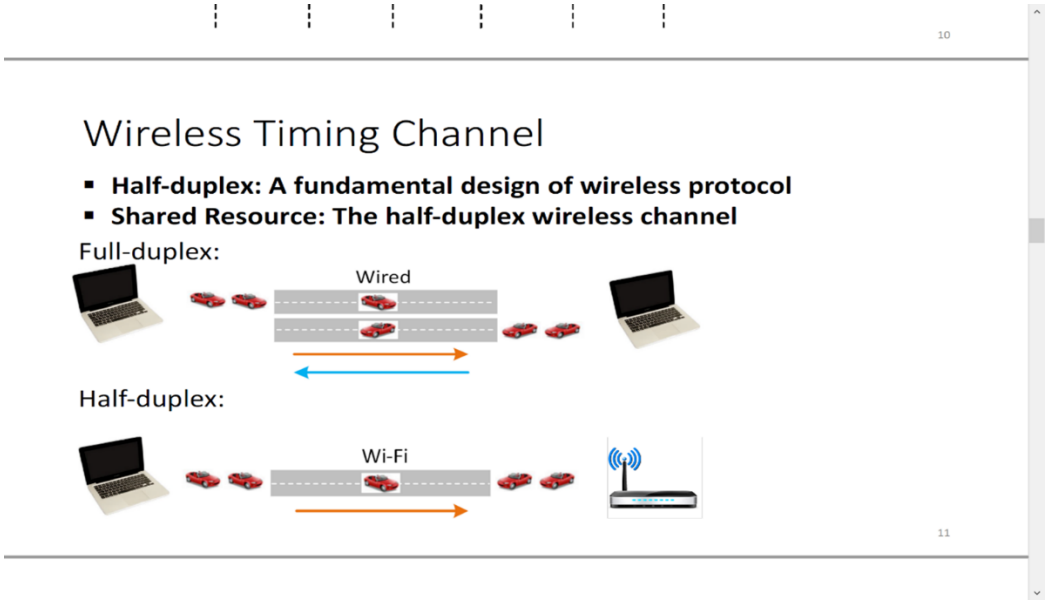
Basically, in order to be attacked by hacker using this flaw, the victim needs to go to the website made by the hacker first. Usually, it could be something like a free football streaming website, a gaming website, or a porn website, all in an effort to lure the victim in there. When the victim stays on that particular website, the website would open another webpage, something important like a bank webpage, without the victim knowing it of course. Then, what it does is that it keeps guessing the sequence number of that important webpage by observing the time interval between receiving a package and giving a reply, employing the unidirectional nature of half-duplex wireless, which Wi-Fi routers currently uses. Then the hacker sent spoofed TCP packets with a the right sequence number, and in the meantime cache it in the browser and asked the browser to directly go to the cache every time the victim goes to that bank website (this is called cache poisoning). In this case, the next time the victim visits the banking website, they will see the malicious copy cached in the browser, and when he types his user name and passwords in, he is basically sending those to the hacker instead of the bank website.

This flaw is extremely harmful, for it exploits the fundamental nature of TCP protocol and Wi-Fi. Therefore, there isn’t really much can be done about it without changing the way we transmit information. Employing full-duplex Wi-Fi technology would be the most straightforward solution However, doing that could be extremely expensive, and it would also be implausible for the half-duplex Wi-Fi routers are too

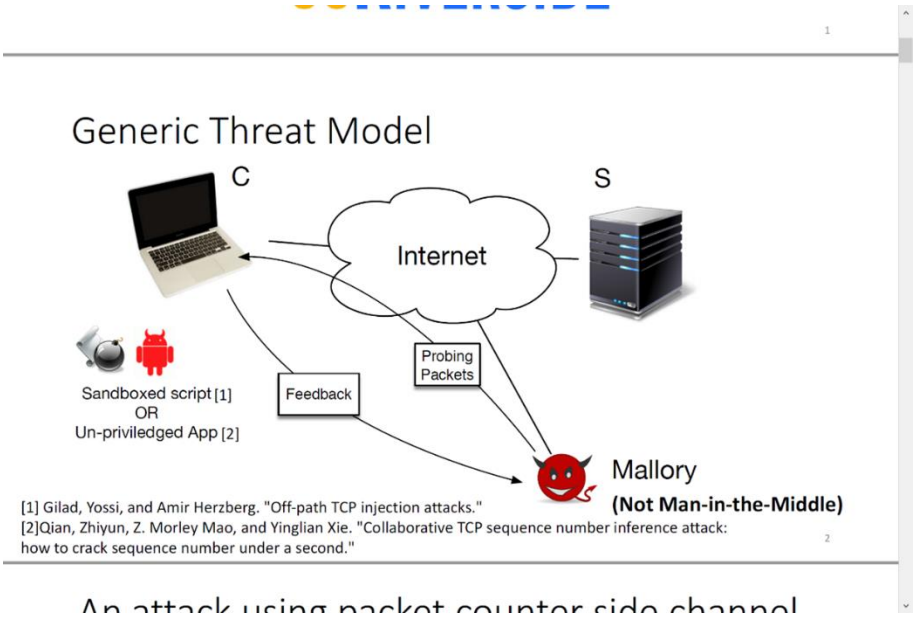
prevalent nowadays to change all of them overnight. Still, there are some things that could done to avoid being attacked using this flaw. For websites, especially important websites like bank websites, one way is to use HTTPS and HSTS instead of HTTP, for the HTTPS and HSTS transmissions are encrypted, and hackers can't just insert a random package in the transmission easily. For common internet users, avoiding going to suspicious websites, like the free sports streaming website or free porn website as described above, would be a very good idea.

More and more flaws originated in the way computer scientists decided to build computers systems and information transmission method like the one this paper talked about would appear in the future. Although the flaw this paper talked about could be fixed, for computer scientists, it's probably a good time to start thinking about developing a new computer system wiping out those flaws, before the day came when our computer got too vulnerable to attacks employing those flaws to do anything at all.

The half-duplex nature of WiFi explained:



How the attack works in a nutshell:



Works cited:

Holly Ober. *New security flaw discovered in Wi-Fi routers*. UC Riverside News

Weiteng Chen and Zhiyun Qian. *Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secrets*. 27th USENIX Security Symposium