Reaction to "ZMap: Fast Internet-wide Scanning and Its Security Applications"

1) Technical details (approach/technique) that you found novel/ Something specific you learned that you didn't know before

The most innovative idea I have seen in this paper is that they are not using traditional way to create persistent connections through TCP/IP stack which requires kernel resource. Instead, they directly create network packet and use libpcap to directly access returned packets. This dramatically reduce the required system resource and overhead necessary to maintain connection status. With this new feature, the authors successfully achieve their goal of doing internet scan using a single entry-level server.

Using an asynchronous stateless manner to receive packet also enable ZMap to avoid timeout setting problems that are often encountered by network scanning tools like NMap.

2)Could I have done this work if I had the idea why or why not?

I could repeat the work as all the information required are published in the paper. It just requires the developers to have sufficient knowledge about network.

3)Is there anything I could do to repeat or validate?

With the open source project, all the things that had been mentioned in the paper can be repeated. However, it should be noticed that they mentioned that because of the scanning operation the authors have received several warning as well as some retaliatory DOS attack. So care should be taken when such tests are conducted.

4) What is my best idea for follow on work that I could personally do?

I am planning to read more about the TCP cache it mentioned in the paper. I am thinking about building a traceroute tool that can collect information from different location of world without the help of traceroute servers. The TCP cache mentioned in the paper, which allows users to carry customized workload in the network packet may be a way to achieve this.

5)What is my best idea for follow on work that I'd like to see the authors do?

I am interested in the future work of scanning IPv6 space mentioned by the user. From the data provided in the paper, it will need around 44 min to scan entire IPv4 space. IPv6 has a far much bigger space than IPv4, thus may require still considerable time, which may makes the idea impractical. However, as IPv6 are not widely used yet, there are still chances to trace the development of IPv6 growth.

6)Any logistical experimental lessons I learned?

The most important lesson I have learned from the paper is that when such kind of research work is conducted, related authorities and school official should be informed in advance. Such

kind of actions may bring unexpected result like the DOS attack that had been mentioned in the paper. Without the support from school it can be very dangerous.

7)How does this compare to the other papers we read? Most similar? How different? Other comparisons?

This paper targets at different aspect comparing to the 2 papers we have read. No comparison is available

8)What is your biggest criticism of the paper?

I don't have much criticism to this paper. The only one is against the remaining ring it used. There's no strong proof that it is truly identically distributed.