CS6353 Assignment 3

Zi Yan

1 Q1

Solution:

(a) Because change other strings may interrupt the protocol, or destroy the exploit semantics. And most exploits are trying to inject a jump address to redirect the control flow of a program.

(b) Because Packet Vaccine does not look at the source code of a program, and never monitor on execution flow of a program, but only the output of a program.

(c) Because these attacks are mainly adopted by attackers, and they are taking advantage of injection of a jump address.

2 Q2

Solution:

(a) Once one sensor is compromised, all the communication channels will be insecure due to the key loss.

(b) First, they broadcast all the identifiers of the keys they have. Second, they pick a key shared by both in their key ring according to the identifiers.

(c) They will find a path between them, which consisted of nodes that can use shared keys to communicate, and then pick a path-key from unused keys in the key ring.

3 Q3

Solution:

(a) The author want to find out whether a single executable contains a spyware or not, without other executables' interference.

(b) Yes. If a scan shows a bunch of executables are clean, those executables do not need to be scanned individually. Therefore, this way can save a lot of time.

(c) Three times. 1) Group all eight in two groups, where each has four. 2) **Scan** one group. If scanned one is clean, separate the other group into two groups, where each has two. Otherwise, separate scanned group into two, where each has two. 3) Pick one group to **scan**, and separate the not clean group as 2). 4) Now, we have two executables left. **Scanning** any of them can tell which one contains spyware.

4 Q4

Solution:

(a) 1) To save storage space by reducing node information (compared to node append), 2) to resist multiple attack paths (compared to node sampling).

(b) To save storage space, because only one segment, offset information and distance will be stored.

(c) 1) For node sampling, it cannot reconstruct the path. 2) For edge sampling, it does not matter.

5 Q5

Solution:

(a) By using MAC of the message and the counter.

(b) They need a master key $\mathcal{X}_{AB}$. For data encryption/decryption keys: $K_{AB} = F_{\mathcal{X}}(1)$, $K_{BA} = F_{\mathcal{X}}(3)$, and for MAC encryption/decryption keys: $K'_{AB} = F_{\mathcal{X}}(2)$, $K'_{BA} = F_{\mathcal{X}}(4)$. And $F_{\mathcal{X}}$ is a pseudo-random function.

(c) The counter is authenticated by MAC, and it will increase monotonically at each communication. So any replay attacks cannot succeed.