HW3 (cs6353)

Submitted by: Prosunjit Biswas

1. (a). If they install multiple executables and spyware is detected then it is hard to conclude which one (or many) of the executable have been infected with spyware.

(b). Yes, it helps to install K executables. Lets assume we have 100 executables and we know < 5% contain spyware. Now if we divide the spyware in 5 groups having 20 executables (k=20 here) in each group. Now, with a single scan we may find that some of the group may not contain any spyware in which case we can discard these executable from further scanning. Again, if we find that each of the 5 group has executable, then we know each group has only one infected executable (using the fact that, < 5% executable are affected). Once, we know one group of executable has only one spyware, we can scan the spyware in binary search fashion.

(c). Binary search technique helps here.

- First divide the executables in 2 groups having 4 executables each. And scan once to see which group has spyware.

- Divide the infected group, with 2 subgroup having 2 executables and scan once more and detect the group having spyware.

- now, we have 2 spyware. Scan any one of the 2 executables to detect the executable having spyware.

1. (a).

- tracking multiple co-ordinated attacker.

- quick convergence of attack path

(b). For accommodating the information in limited packet space.

(c). If each router marks with different probability which is not known to the victim, he cannot

reconstruct attack path.

1. (a). Authentication is done by generating MAC.

(b). The two communicating parties A and B share a master secret key, and they derive independent

keys using the pseudorandom function

( c). Replay attack is detected by using the counter with each sensor (weak freshness).

1. (a). when a user joins or leaves a group, it trigger a change in the group key.

(b). In star topology, when a new user joins, the group key is unicasted to him using his own shared key with the keycenter.

(c). No, it is not possible to have cycle in key graph - because there is no edge from key to user. To have a cycle, there needs both types of edges – user2key and key2user.

1. (a). It may not help having more than one tool. For example, if the tools share phishing feed and detection techniques, there will be on improvement in detection.

(b). When a legitimate site is blacklisted as phishing site, then some phishing tools who use only phishing feeds for detection may detect the legitimate site as phishing site.

(c). to avoid being blacklisted by their domain or address.

1. (a). number of e-mail send to a domain is used in behavioral blacklisting. More specifically, domain X # send email X time is used for behavioral blacklisting.

(b). By clustering, we can easily classify new spamming domain to corresponding category.

(c). For every new spam domain, the approach combine the the domain to a existing cluster which eventually change the behavior of the cluster over time. This is how, new sending pattern is adopted.