4.1.2 Dynamic Protocol Decoder

The IP addresses within the infrastructure is generated in a dynamic and randomized method, which means that in every protocol, every endpoint will hold a new identification number different to that of regular IP addresses. The actual identification for every host is shuffled with the sequence of bits within packets. Every host obtains its new identification number from the dynamic protocol decoder based on the randomization function that ensures how the new IP address is structured in the reformed packets [1].

The dynamic protocol decoder is responsible for a count of all endpoints inside an infrastructure and then forming a new connection graph that consists of all these endpoints. The dynamic protocol defines the communication sequence between all nodes, the number of fragment required and the arrangement of bits inside these packets [1].

4.1.3 Understanding Agent

The understanding agent controls incoming and outgoing traffic in all endpoints. One of the main tasks of the understanding agent is to receive the ambiguous packets and decode it back to the original (TCP/IP or OSI network protocols), which is necessary for upper layers in the original network protocols. This concept is employed to avoid major changes in the upper layers (above the network layer) [1].

4.1.4 Monitor Engine

The monitor engine in our approach is the decision maker, which is basically made for intrusion detection. Generating decision by monitor engine is heavily relied on the generated dynamic protocol by the dynamic protocol decoder. The detection mechanism is simple, if an endpoint repeatedly does not comply with the current dynamic protocol; it is an intruder [1].

5. Demonstration of the approach work

It is important to show a scenario of the approach in practice. The figure shows the architecture of a network with our approach. The network setup won't get affected since the approach has been designed in respect to existing technologies including OSs, routers, servers or even network cables [1].

In fig. 7, the understanding agents are connected to every host inside the infrastructure. Also, a one understanding agent is connected to every router inside the network. The only possible way for all hosts, servers and routers to communicate properly is by the understanding agents since this approach performs its tasks on packet level.

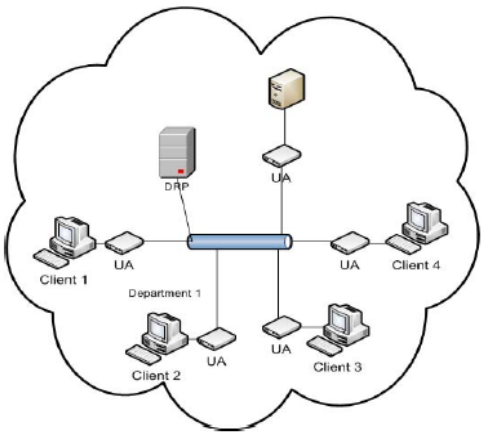

Figure 7: A network with approach's components

Fig.8 illustrates the understanding agents' main function between a client and server via a router. The dynamic protocol decoder generates the new communication protocol based on the fundamentals and concepts illustrated in the previous sections. Then, it distributes the new protocol to all nodes integrated with the network and these new protocols must be encrypted. After that, understanding agents decrypt that massage and function in the respect to the new generated protocol.

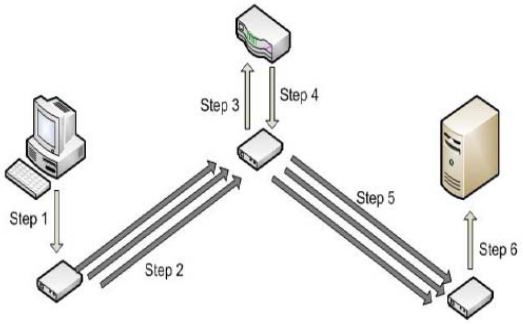

Figure 8: Understanding agents main functions

Figure 9 illustrates the actual physical network setup; however, the virtual communication between these nodes is different, see figure 6. For example, in order for client 2 to communicate with server 5; the client 2 must follow the structure of the trusted graph and the dynamic protocol which enforces client 2 to go throw the client 3 and then to the server 5 and vice versa. So the physical communication will be in that sequence. First, client 2 sends a request to server 5. The actual request is generated normally by the OS in client 2 without any interference from its understanding agent. Then, the understanding agent for client 2 obtains that request before it goes to the network cable. The understanding agent right now reforms the packet into the current communication protocol (dividing the original packet into more than one packets, shuffled up packets 'bits, hiding the identity of the host itself) generated by dynamic protocol decoder. After that, the understanding agent for client 2 sends these packets normally to the router.

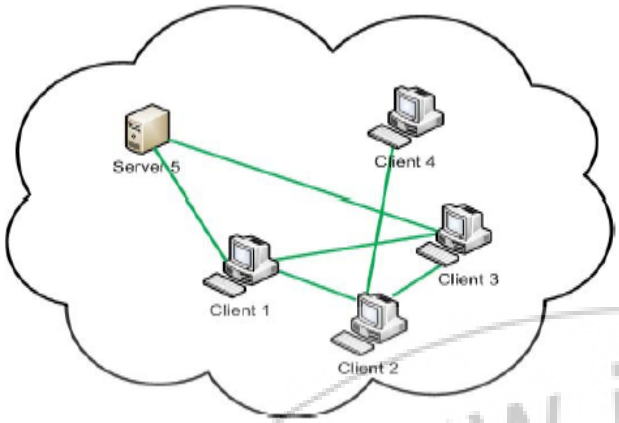

Figure 9: Connection

The understanding agent for the router receives these packets and based on the trusted graph the understanding agent for the router resends these packets to client 3 with little bit of confusion. If the understanding agent for the router redirects messages directly to the next node in the graph, hackers can easily identify the architecture of the trusted graph. So, the understanding agent for the router sends these packets to its destination with extra packets to some nodes for confusion purpose. Subsequently, the understanding agents for client 3 receives the divided packets originally sent by client 2 and recognizes that theses packets are directed to server 5; so, the understanding agent for the client 3 resends these packets to the router again. The same step illustrated before when the understanding agents for the router receives the packets from client 2, is performed again by the router's understanding agent but the packets are directed to its destination (server 5) with the same confusion concept.

Now the understanding agent for server 5 receives these packets and from their formation, the understanding agent reforms these packets into its original form (exactly like what client 2 generates before but it has been modified by the understanding agent for client 2). After reforming it again, server 5 receives this request and replies to it normally. These communication steps are performed again for the reply generated by server 5 to its final destination client 2.

Hence, this approach provides a complex communication infrastructure [1].

6. Conclusion

The proposed system is to develop a conceptual dynamic security approach against hacking in general. This approach is also constructed to target the three essential pre-hacking steps, which results on launching an attack against infrastructures practically complicated. It facilitates communication within the infrastructure in a most confused method. Therefore, it is impossible for hacker to form hacking strategies because of confusion and thus nearly impossible to perform any task. This approach is a new security solution compared with its own kind.

References

[1] Saad Alsunbul, Phu Le,Jefferson Tan "A defense security approach for infrastructures against hacking", 2013 IEEE DOI 10.1109/TrustCom.2013.197, pp.1600-1606.

[2] B. Smith, Yurcik, W., Doss, D., "Ethical hacking: the security justification redux," in *Technology and Society, 2002. (ISTAS'02). 2002 International Symposium on*, 2002, pp. 374-379.

[3] A. X. Liu and M. G. Gouda, "Firewall Policy Queries," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 20, pp. 766-777, 2009.

[4] *B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "*Network intrusion detection,*" Network, IEEE, vol. 8, pp. 26-41, 1994.*

[5] M. Sourour, B. Adel, and A. Tarek, "Environmental awareness intrusion detection and prevention system toward reducing false positives and false negatives," in *Computational Intelligence in Cyber Security, 2009. CICS '09. IEEE Symposium on*, 2009, pp. 107-114.

[6] L. Spitzner, "The Honeynet Project: trapping the hackers," *Security & Privacy, IEEE*, vol. 1, pp. 15-23, 2003.

[7] Wenjun Jiang, Guojun Wang, Jie Wu, "Generating trusted graphs for trust evaluation in online social networks", 2012 Elsevier, doi:10.1016/j.future.2012.06.010.

Author Profile

Prof. D. N. Rewadkar Prof. D. N. Rewadkar received M.E. Computer Technology, from S.R.T.M. University, Nanded. (2000). Currently he is working as an Associate Professor & Head the Department of Computer Engineering, in RMD Sinhgad Technical Institutes Campus, Warje, Pune. He was a Member of Board of Study (BOS) committee of S.R.T. Marathwada University, Nanded for Computer Science & Engineering. His area of interest is Traffic Engineering & Mobile Communication. He has 21 years of teaching experience.

Harshal A. Kute Reseach Scholar RMD Sinhgad School of Engineering, University of Pune. He has received B.E. in Information Technology from Information Technology department of Sinhgad College of Engineering from University of Pune, Pune (2013). Currently he is pursuing M.E. in Computer Engineering from RMD Sinhgad School of Engineering, Warje, Pune, University of Pune.