MilSeg: SDN-based Military Network Segregation Architecture

Kwang Joon Yang, Jinho Choi, Seungsoo Lee and Seungwon Shin

May 9, 2019

MilSeg: SDN-based Military Network Segregation Architecture

Kwang Joon Yang, Jinho Choi, Seungsoo Lee, Seungwon Shin*
Graduate School of Information Security
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea
dsider, cyberz, lss365, *claude@kaist.ac.kr

I. Introduction

Software-Defined Networking (SDN) is widely used by a number of companies (e.g., Google [1]) for the various advantages such as centralized network management, dynamic control efficiency, and enhanced security management [1]. Especially, with the centralized network control that SDN offers, SDN is also utilized and studied in the military networks of major countries [2], [3], including the United States, however, there is a lack of research that improves the security of military networks through SDN. Generally, closed organizations like the military have several problems that are the ordinary perimeter defense-centric design, blacklisting-based security policies, and limited protection capabilities to the endpoint.

For dealing with those problems, in this study, we propose a new architecture called `MilSeg` that *segregates* military networks in the SDN environment in order to minimize various attack vectors and spread of damage from the attacks targeting the military networks. And, the major features MilSeg has are as follows:

(1) Whitelisting-based security policy grouping and optimization by using pre-defined user attributes in the military.

(2) Network traffic segregation by applying the enhanced network access control list to the end switch (the advantages of SDN) in accord with purposes of military.

(3) Dynamic secure path allocation that guarantees anonymity, security and flexibility in the network.

II. System Design of MilSeg

MilSeg is basically based on SDN architecture, and it groups policies by the attributes of hosts to facilitate the whitelisting policies while detailed parceling traffic out from the inner network viewed at a zero trust perspective.

Figure 1 shows an overall system design of MilSeg, which consists of three main components; 1) segregation components, 2) secure forwarding components and 3) the other external components. Each component is respectively highlighted in green (segregation) and red (secure forwarding) colors from a functional point of view. The segregation components (green) are responsible for the segregation mechanism which is a key feature of MilSeg, and the secure forwarding components (red) perform a secure packet forwarding that guarantees dynamic connectivities between the segregated networks stably.

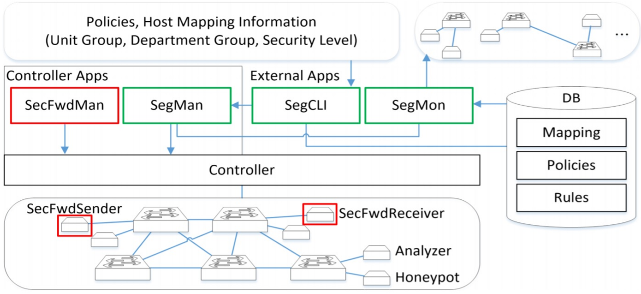

Fig. 1. Overall System Design of MilSeg

III. Segregation and Secure Forwarding Mechanism

The segregation mechanism is the key part of parceling out network traffic by interconnecting between each segregation component in MilSeg, and it can be classified into 3 stages as shown in Figure 2.

(1) First, `SegCLI`, which is the interface between the administrator and `SegMan`, receives a grouped policy based on the host's attribute information that is predefined by the essentiality of military, including the host's units, departments, addresses, security level and functional authority.

(2) Next, the policy is converted into a type that SegMan can understand and the number of the policy is minimized by the policy optimization.

(3) SegMan translates the optimized policy into the flow rules and installs them on the appropriate end switches.

From those segregation steps, the network traffic is subdivided by the policy, and `SegMon` delivers the segregation results and statistic information to the administrator.

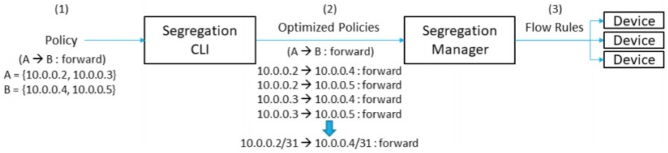

Fig. 2. Example of the Segregation Mechanism

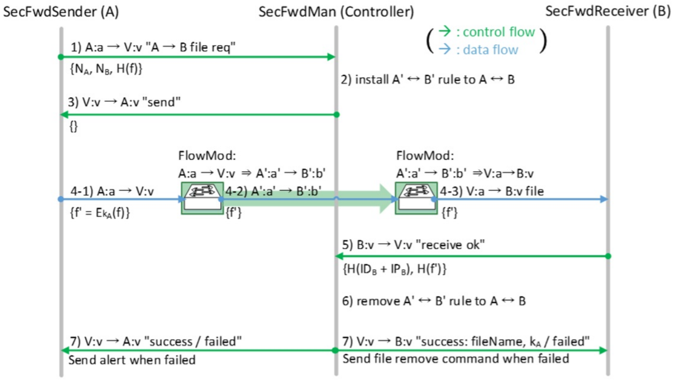

Fig. 3. Example of Secure Forwarding Procedure

There are two types of the policy; basic and normal. The basic policy defines how to control each host in the intersection to assist with the whitelisting policy.

Meanwhile, the normal policy is similar to the access control list (ACL) policy, but it can be represented by grouping hosts according to the host addresses. Also, the normal policy can add some advanced actions to the packets; i) a redirect action, which transfers the packets to the destination host and blocks existing connections. ii) a redirect and forward action, which allows both redirect and existing connections. iii) a honeypot action, which modifies packet header information for connection with the honeypot in order to inspect the network traffic for military purposes.

The secure forwarding component provides a secure connection between the segregated network by the policy without adjusting the configuration. In this way, it is possible to fundamentally improve the method of secret documents management in the military networks. The detailed procedure is shown in Figure 3.

1) The connection between `SecFwdSender (A)` and `SecFwdReceiver (B)` has been blocked by the segregation. The sender sends a transfer request with a concatenated value (A position, B position, the hash value of the file) to the agreed temporary address (V:v) without knowing of the real address. The request is delivered to `SecFwdMan` according to the pre-installed flow rule. 2) After the SecFwdMan gets the request, it authenticates the sender with the port information receiving from the switch and validates if the request is legal or not (i.e., whether the file is owned or not, security levels). If the request is allowed, the flow rules hiding the addresses A and B as A' and B' are installed on each switch as a secure path that can protect from the side channel attack by providing the anonymous. 3) After installing the flow rules, the SecFwdMan tells the sender that the transfer is approved and ready. 4) The sender encrypts and forwards the file to the receiver through the switches. 5) The receiver reports the results of the file receipt to the SecFwdMan. 6) Based on the results, the SecFwdMan deletes the temporary flow rules (A' and B') installed for the security. 7) Finally, the SecFwdMan informs A and B of the results respectively. If problems occur in this transferring process (e.g., file integrity corruptions or network attack detections), the targeted hosts can be denied by the segregation component.

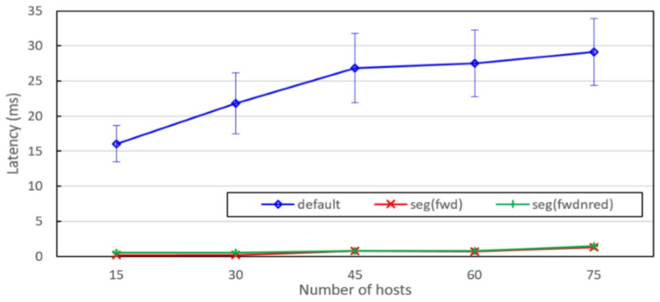

Fig. 4. Performance Evaluation Results of Segregation Component: Comparing the initial flow latency

IV. Performance Evaluation

Figure 4 shows the results of the performance evaluation of the segregation component, and for the measurements, we change the number of the hosts that are connected to 15 switches except for the center switches. While the existing reactive forwarding application (control group) brings the delay more than 15 ms for the initial flow, the segregation component in MilSeg (both forward and forward & redirect actions) has the delay of at least 10 ms less. This could not be a significant benefit on average, but it has a positive effect on the user level to decrease the initial connection delay. After the initial flow, the latency is almost similar to that of the control group.

V. Conclusion and Future Work

In this paper, we propose MilSeg, a network segregation architecture for enhancing the military networks, and we show its applicability through the system design and the performance evaluation results. To improve the efficiency as well as the security of the military networks, we adopt SDN concept into the networks, so it can be consistent with the efficiency of National Defense Reform and the aspects of future warfare. And, we also look forward to further advancing this study by supplementing the policy optimization to handle the flow rule conflict, and by adopting network virtualization so that policy optimization can be applied in all cases. Therefore, it is expected to motivate the related research and to improve the security of the tactical network on the battlefield.

References

[1] S. Shin, H. Wang, and G. Gu, “A first step toward network security virtualization: From concept to prototype,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2236–2249, 2015.

[2] MilCloud. [Online]. Available: http://www.disa.mil/computing/cloud-services/milcloud

[3] K. Phemius, J. Seddar, M. Bouet, H. Khalifé, and V. Conan, “Bringing sdn to the edge of tactical networks,” in *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE, 2016, pp. 1047–1052.