2020 한국차세대컴퓨팅학회
하계학술대회

장　　소 : 제주 JDC(엘리트빌딩)

일　　시 : 2020. 8. 20(목) 14:00 ~ 8. 22(토) 12:00

주최 · 주관 : 한국차세대컴퓨팅학회, 제주드론산업협회

송신 IP 암호화를 통한 미션 크리티컬 시스템 트래픽 분석 방해 기법

Traffic Analysis Obstructing Scheme for Mission-Critical System by Encrypting Source IP

이양재[1], 박기웅[2,*)]

Yangjae Lee, Ki-Woong Park

[1](05006) 서울시 광진구 능동로, 세종대학교 시스템 보안 연구실

[2](05006) 서울시 광진구 능동로, 세종대학교 정보보호학과

leelambjae@gmail.com[1], woongbak@sejong.ac.kr[2]

요 약

인터넷의 활용이 증가하면서 네트워크 트래픽 또한 증가하고 있다. 우리는 일상적으로 웹사이트나 외부 시스템에 접속하여 수많은 패킷을 주고받고 있다. 하지만 네트워크 트래픽의 증가는 공격자에게도 이점을 안겨주었다. 일반적으로 우리는 패킷에 담아 전송하는 데이터를 보호하기 위해 암호화를 사용한다. 공격자는 암호화된 데이터를 목표로 하는 대신 부수적으로 획득할 수 있는 패킷 간의 간격, 패킷 크기, 패킷 헤더 분석을 통해 통신 상태 확인, 송수신자 식별 등의 정보를 획득할 수 있다. 미션 크리티컬 시스템에서 공격자는 트래픽 분석으로 얻은 정보를 바탕으로 통신 상태를 확인할 수도 있고, 다음 공격 수행을 위한 초석으로 삼을 수 있다. 본 논문에서는 패킷 분류의 핵심이 되는 Source IP를 암호화하여 패킷 분류를 방해함으로써 어렵게 공격자의 트래픽 분석 난도를 높였다.

키워드: 미션 크리티컬 시스템, 트래픽 분석, TCP/IP, 네트워크 보안

1. 서론

미션 크리티컬 시스템은 조직 운영에 핵심적인 역할을 수행한다. 따라서 미션 크리티컬 시스템은 보안 사고가 발생할 경우 조직에 막대한 피해를 입힐 수 있어 신중한 관리 및 보안이 요구된다[1,2]. 미션 크리티컬 시스템을 함락시키기 위해 공격자는 지속적으로 여러 루트로 동시다발적으로 공격을 수행한다[3]. 공격자는 미션 크리티컬한 군 통신 네트워크에서에서 트래픽을 가로채 군용 기기들의 신호를 확인하거나 통신 중인 송 수신자를 식별할 수 있다 [5]. 트래픽 분석 공격은 패킷의 헤더와 패킷 간의 간격[6], 패킷 속도[5] 등을 분석하기 때문에 패킷 암호화는 트래픽 분석을 위한 방안이 아니다. 이러한 트래픽 분석을 방지하기 위해 많은 연구가 진행되고 있다. Feghhi는 적극적인 공격자가 인식 가능한 패턴을 트래픽에 포함하여 패킷의 흐름을 분석하는 것을 방지하기 위해 디지털 필터링 기술을 제안하였다[6]. Haipeng Qu는 노이즈가 있는 비밀 채널을 생성하여 비밀 정보를 교환할 수 있도록 하여 공격자의 분석을 방해하였다[7]. Cai는 패킷의 크기를 기반으로 트래픽을 분석하는 방식을 막기 위해 패킷에 패딩을 삽입하여 공격자의 트래픽 분석을 방해하였다[8]. RAHBARI는 논문에서 패킷 헤더의 MAC 주소를 난독화하여 공격자의 트래픽 분석을 방지하는 방안을 기술하였다[9]. 하지만 아직 패킷의 Source IP를 감추는 연구는 거의 진행되지 않았다. Source IP는 공격자가 트래픽을 분석

* 교신저자

하는데 있어 중요한 정보로[4] Source IP를 숨김으로써 트래픽 분석의 난이도를 더욱 높일 수 있다. 하지만 Source IP를 변조하는 것은 해결해야할 문제가 있다.

첫 번째로 패킷의 Source IP가 변조될 경우 미션 크리티컬 시스템은 응답할 목적지를 정의할 수 없기 때문에 사용자는 응답을 받을 수 없다. 본 논문에서 사용자 에이전트와 미션 크리티컬 시스템은 암호화 및 복호화를 위한 키를 사전에 교환하여 Source IP를 암호화 및 복호화 할 수 있도록 하였다. 하지만 이때 일반적인 암호화를 사용할 경우 Source IP와 암호문이 1:1 대칭이 되어 공격자가 암호문과 사용자를 매핑할 수 있어 공격자로부터 트래픽 분석 공격을 방지하는데 큰 효과가 없다. 이를 극복하기 위해 본 논문에서는 사용자가 Source IP와 Tag를 사용해 서로 다른 암호문을 만들 수 있도록 하였고, 미션 크리티컬 시스템은 서로 다른 암호문에서 Tag와 키를 사용해 동일한 Source IP를 획득할 수 있도록 하였다. 이를 통해 공격자는 복수개의 암호문에서 사용자를 특정할 수 없어 트래픽 분석이 어려워진다.

두 번째로 Source IP를 암호화 및 복호화 하는 계층을 고려해야 한다. 이 문제는 Source IP를 패킷 데이터에 삽입 후 데이터를 암호화함으로써 Source IP를 노출하지 않으면서 문제를 해결할 수 있다. 하지만 데이터 안의 Source IP를 복호화 하기 위해서는 Source IP가 삽입된 데이터 계층이 복호화가 될 때까지 미션 크리티컬 시스템이 Source IP를 알 수 없다는 문제가 있다. 네트워크 계층에서 Source IP를 기반으로 패킷을 필터링하는 방화벽의 경우, 암호화된 Source IP로 패킷 필터링을 할 수 없으므로 정상적으로 작동할 수 없다. 따라서 본 논문에서는 IP 기반 패킷 필터링 방화벽을 사용할 수 있도록 고려하였다. 본 문제를 해결하기 위해 Source IP를 암호화하지만, 암호화된 Source IP와 Tag를 네트워크 헤더에 삽입함으로써 미션 크리티컬 시스템의 네트워크 계층에서 사용자의 Source IP를 복호화 할 수 있도록 하였다.

세 번째로 패킷 크기의 증가를 최소화하여 데이터의 통신 지연을 최소화하여야 한다. 암호화된 Source IP를 데이터에 삽입할 경우 패킷의 크기가 커진다. 때문에 패킷에 데이터를 삽입할 공간이 줄어들어 데이터 전송 속도가 감소한다.

Source IP 변조를 통한 본 논문의 기여는 다음과 같이 요약할 수 있다.

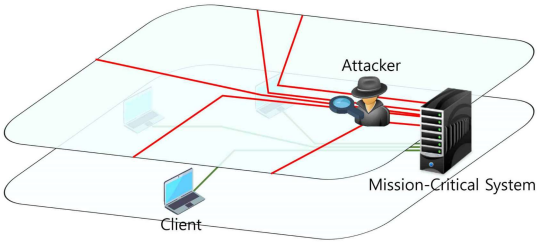
첫 번째로 공격자의 트래픽 분석 난이도를 높이기 위해 트래픽 분석에 핵심 요소인 Source IP를 암호화하였다. 이때 공격자가 암호문과 Source IP를 1:1 매핑하는 것을 방지하기 위해 동일한 Source IP로 복수개의 암호문을 생성할 수 있도록 구현하였다.

두 번째로 OSI 7 계층 기준으로 Source IP 복호화를 네트워크 계층에서 수행할 수 있도록 함으로써 Source IP 기반 패킷 필터링 방화벽을 사용할 수 있도록 구현하였다.

세 번째로 패킷 헤더 크기의 증가를 최소화하여 데이터 전송 시 발생하는 지연을 최소화하였다.

본 논문의 구성은 다음과 같다. 2장에서는 트래픽 분석 방해 기법의 디자인을 설명한다. 3장에서는 트래픽 분석 툴의 패킷 분석 요소를 정리하여 Source IP를 알 수 없을 경우, 트래픽 분석 난이도 상승됨을 보인다. 마지막으로 4장에서는 결론을 기술한다.

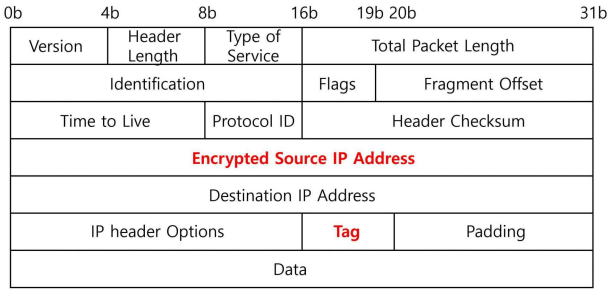
2. Design



(그림 1) Traffic Analysis Obstructing Overview

본 메시지 교란 기법의 핵심 요소는 하나의 Source IP를 복수개의 암호문으로 암호화하여 공격자의 트래픽 분석의 난이도를 상승시키는 것이다. 공격자는 복수개의 암호화된 Source IP에서 사용자를 특정할 수 없어 트래픽 분석의 난이도가 상승하여야 한다. 또한 IP 기반 패킷 필터링 방화벽을 지원하며 패킷의 지연을 최소화하기 위하여 암호화 및 복호화가 네트워크 계층에서 수행되어야 하며, 패킷 헤더의 크기 증가를 최소화 하여야 한다.

이를 구현하기 위해 본 기법에서는 IP 헤더의 일부



(그림 2) IP Header for Traffic Analysis Obstructing

를 수정하였다. 사전에 사용자 인증 과정에서 미션 크리티컬 시스템은 인증이 완료된 사용자에게 키를 전달한다. 이때 사용되는 키는 사용자 식별 절차 없이 복호화를 위해 모든 사용자가 동일하다고 가정한다. 암호 방식은 구현 방식에 따라 Tag를 사용하는 다양한 공개키 암호화를 사용할 수 있다. 사용자는 키와 Tag를 사용하여 Source IP를 암호화하고 IP 패킷 헤더에 암호화된 Source IP와 Tag를 (그림 2)의 IP 헤더에 삽입한다. 공격자는 공개된 Tag에서 소량의 정보를 획득할 수 있지만 Tag는 여러 사용자가 중복하여 사용하기 때문에 사용자 매핑은 여전히 난도가 높다. 예를 들어 한 명의 사용자가 16개의 Tag를 사용할 때, 암호화된 Source IP가 다르더라도 Tag가 유일하기 때문에 공격자는 패킷과 사용자를 매핑할 수 있다. 하지만 사용자가 두 명이 될 경우 Tag가 중복되기 때문에 공격자는 패킷의 Tag가 어느 사용자의 것인지 알 수 없다. 이는 사용자가 증가할수록 Tag의 중복 또한 증가하기 때문에 분석을 보다 지연시킬 수 있다.

미션 크리티컬 시스템은 패킷을 수신한 뒤, 네트워크 계층에서 Tag를 읽어 암호화된 Source IP를 복호화 한다. 이 과정에서 암호화된 Source IP와 Tag가 IP 헤더에 존재하기 때문에 네트워크 계층 방화벽은 복호화 된 Source IP를 기반으로 IP 필터링을 수행할 수 있다. 이를 통해 빠르게 패킷을 필터링할 수 있어 자원을 보다 효율적으로 사용할 수 있게 된다.

3. Evaluation

본 절에서는 트래픽 분석 툴이 Source IP를 알 수 없을 경우 트래픽 분석이 원활하게 이뤄지지 않음을 보이기 위해 네트워크 트래픽을 분석을 위해 기록하는 패킷의 대표적인 요소들을 표로 정리하였다.

<표 1> Traffic Analysis Tools Flow Record Format

Traffic Analysis Tool	Source IP	Source Port	Destination Port	Protocol	TTL	Packet Length
Azure Network Watcher [10]	○	○	○	○	X	X
CoralReef [11]	○	○	○	○	X	X
NetFlow [12]	○	○	○	○	○	○
Corsaro [13]	○	○	○	○	○	○

<표 1>의 CoralReef, Netflow, Corsaro 같은 트래픽 분석 툴은 Flow Type에 기반하여 [14] 네트워크의 트래픽을 분석한다. Azure Network Watcher[10], CoralReef [11]의 경우 5-tuple을 사용하여 패킷의 Source IP, Source Port, Destination IP, Destination Port, Protocol을 기록하였다. 또한 NetFlow[12]와 Corsaro[13]의 경우 8-tuple을 사용하여 추가적으로 Time To Live(TTL), Packet Length, TCP Flags를 기록하였다.

<표 1>에서 트래픽 분석 툴이 기록하는 패킷 요소에서 볼 수 있듯이 대부분의 트래픽 분석 툴은 Source IP를 기록하여 분석에 사용한다는 것을 알 수 있다. 트래픽 분석 툴에 정상적인 Source IP가 기록되지 않는다면, 트래픽 분석 툴은 정상적으로 트래픽 분석을 못할 것이다. Source IP를 필요로 하지 않는 분석 툴이 개발되더라도 사용자와 패킷을 매핑 시키는데 많은 연산을 필요로 해 일반 분석 툴에 비해 속도가 느릴 것으로 예상된다.

4. Conclusion

본 논문에서는 공격자가 미션 크리티컬 시스템과 사용자 간 암호화된 통신을 하더라도 숨길 수 없는 정보를 기반으로 트래픽을 분석하는 것을 방지하고자 트래픽 분석 방해 기법을 제안하였다. 동일한 Source IP는 Tag에 의해 복수개의 암호문으로 암호화되기 때문에 공격자에게는 사용자 한 명의 패킷이 마치 수십 명이 보내는 것과 같이 보인다. 트래픽 분석 방해 기법은 공격자가 사용자와 미션 크리티컬 시스템을 매핑 시키는 것을 방지해 트래픽 분석을

방해한다.

본 논문에서 제안한 기법을 통해 공격자의 트래픽 분석 난이도를 높일 수 있으며 IP를 기반으로 패킷을 필터링하는 방화벽을 운용할 수 있다. 또한 암호화된 Source IP를 네트워크 헤더 Source IP 필드에 삽입함으로써 데이터에 삽입했을 경우보다 패킷의 증가를 최소화하였다.

본 논문에서 제안한 트래픽 분석 방해 기법은 미션 크리티컬 시스템에서 트래픽 분석을 어렵게 하는 방어 기법으로 활용할 수 있을 것으로 기대된다.

Acknowledgement

본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2018-0-00420, No.2019-0-00273) 및 한국연구재단 연구과제(NRF-2020R1A2C4002737)의 지원을 받아 수행된 연구임.

참고문헌

[1] 남기효, 김윤홍, 권환우 “최신 정보보호 기술 동향: APT 및 그 대응”, 주간기술동향, 2011. 9. 16

[2] D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, “Security for Industrial Communication Systems,” Proceedings of the IEEE, vol. 93, no. 6, pp. 1152 - 1177, Jun. 2005.

[3] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D., “A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities.” IEEE Communications Surveys & Tutorials, 21(2), 1851-1877. 2019.

[4] CALLADO, Arthur, et al, “A survey on internet traffic identification.” IEEE communications surveys & tutorials, 11.3: 37-52. 2009.

[5] FU, Xinwen, “On traffic analysis attacks and countermeasures” Texas A&M University. PhD Thesis. 2007.

[6] Feghhi, S., & Leith, D. J., “A web traffic analysis attack using only timing information” IEEE Transactions on Information Forensics and Security, 11(8), 1747-1759, 2016

[7] QU Haipeng, SU Purui, FENG Dengguo, “A typical noisy covert channel in the IP protocol” In: 38th Annual 2004 International Carnahan Conference on Security Technology, IEEE, pp. 189-192. 2004

[8] Cai, X., Zhang, X. C., Joshi, B., & Johnson, R., “Touching from a distance: Website fingerprinting attacks and defenses” In Proceedings of the 2012 ACM conference on Computer and communications security. pp. 605-616 2012. 10.

[9] RAHBARI, Hanif; KRUNZ, Marwan “Secrecy beyond encryption: obfuscating transmission signatures in wireless communications” IEEE Communications Magazine, 53.12: 54-60. 2015

[10] Microsoft Network Watcher, https://docs.microsoft.com/ko-kr/azure/network-watcher/traffic-analytics

[11] KEYS, Ken, et al. “The architecture of CoralReef: an Internet traffic monitoring software suite” In: Passive and active network measurement workshop (PAM). 2001.

[12] 박정숙, et al. “플로 기반의 인터넷 트래픽 측정 기술 동향.” 2004.

[13] IGLESIAS, Félix; ZSEBY, Tanja. “Modelling IP darkspace traffic by means of clustering techniques.” In: 2014 IEEE Conference on Communications and Network Security. IEEE, p. 166-174. 2014

[14] NIRANJANA, R.; KUMAR, V. Anil; SHEEN, Shina. Darknet “Traffic Analysis and Classification Using Numerical AGM and Mean Shift Clustering Algorithm.” SN Computer Science, 1.1: 16. 2020.