기업환경에서 SSL 트래픽 검사 메커니즘에 관한 연구

윤지훈, 원유재*
충남대학교 컴퓨터공학과
e-mail:yjh6569@cnu.ac.kr

A Study on Mechanism for SSL Traffic Inspection in an Enterprise Environment

Jihoon Yoon, Yoojae Won*
Dept of Computer Science and Engineering,
Chung-Nam National University

요 약

최근 기업 네트워크에서 암호화 트래픽 사용량이 증가하고 있으며, 악성 행위를 암호화하여 보안 장비를 우회하는 문제들이 발생하고 있다. 본 논문에서는 기업 네트워크 환경에서 암호화된 트래픽을 검사하기 위해 SSL 트래픽을 복호화하는 시스템을 제안한다. 제안하는 시스템은 암호화 트래픽 분석을 통해 악성 행위 및 기업 내부정보 유출 탐지에 활용할 수 있다.

1. 서론

최근 기업 네트워크에서 암호화 트래픽이 차지하는 비율은 증가하는 추세이다. 기업 보안 담당자를 대상으로 조사한 보고서에 따르면 전체 기업 네트워크 중 암호화 트래픽이 차지하는 비율이 25%인 기업이 87%이며, 전체 기업 중 97%가 향후 2년 이내에 트래픽 암호화의 비중을 늘릴 계획이 있다고 응답했다[1].

현재 암호화 트래픽은 네트워크 보안 강화의 수단으로 사용되고 있지만, 보안 전문가들은 암호화된 트래픽이 악성 공격 탐지를 우회하는 수단으로 사용될 수 있음을 경계하고 있다. 사이버 공격에 대한 조사 자료에 따르면 2017년까지 사이버 공격의 50% 이상이 SSL 트래픽을 통해 이루어질 것이라고 예상한다[2]. 사이버 범죄조직 및 해커들은 트래픽 암호화를 내부망 침입, 악성코드 배포, C&C 트래픽 전송에 사용하며, 이러한 악성 행위는 기존 보안 솔루션의 패킷 필터링, 트래픽 검사 등을 우회할 수 있다. 또한, 암호화 통신을 제공하는 일반 사이트가 악성코드에 감염된 경우에도 정상적인 암호화 트래픽을 통해 악성코드가 전달되기 때문에 기존 보안 솔루션에서 악성 행위가 탐지되지 않는다.

본 논문에서는 이러한 문제를 해결하기 위해 기업의 네트워크 환경에서 SSL 트래픽 복호화를 통해 암호화된 트래픽에 포함된 내용을 검사할 수 있는 시스템을 제안한다. 논문의 구성은 다음과 같다. 2장에서는 암호화 트래픽 분석과 관련된 기존 연구를 소개하고, 3장에서는 SSL 보안 통신 방법을 설명한다. 4장에서는 본 논문에서 제안하는 SSL트래픽 분석 시스템의 구조와 동작을 설명한다. 마지막으로 5장에서는 향후 연구 계획을 설명하고 결론을 맺는다.

2. 관련 연구

암호화 트래픽 분석은 암호화 통신과정에서 발생하는 트래픽, 클라이언트의 수정 등을 이용하여 암호화된 트래픽의 내용을 분석하는 방법이다. 암호화 트래픽 분석 방법에는 클라이언트의 User-Agent와 응용에서 제공하는 Cipher Suites 정보를 이용하여 암호화 통신의 위험도를 분류하는 방법[3]과 VPN 환경에서 비밀 공유 스키마를 이용하여 암호화 트래픽을 분석하는 방법이 있다[4].

User-Agent와 Cipher Suites 정보를 이용하여 암호화 통신의 위험도를 분류하는 방법은 서버-클라이언트 통신 간 전달되는 트래픽을 이용한다. User-Agent 정보는 HTTP 통신과정에서 HTTP 헤더를 통해 수집하고, Cipher Suites 정보는 HTTPS 통신의 SSL Handshake 과정에서 Client Hello 메시지를 통해 수집한다. User-Agent와 Cipher Suites 정보는 한 쌍의 사전 형태로 관리하며, 대량으로 수집된 사전정보를 이용하여 안전한 암호화 통신과 취약한 암호화 통신으로 분류한다. 새로운 HTTPS 통신이 발견되는 경우, 수집된 사전 정보의 User-Agent,

* 교신저자

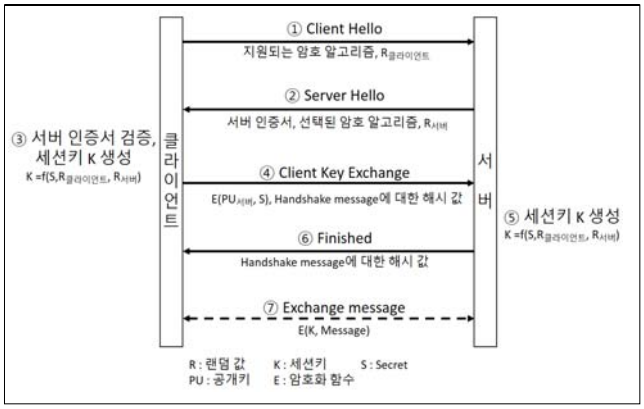
Cipher-Suites 정보와 암호화 통신의 정보를 비교하여 통신의 위험도를 판단한다. 암호화 통신 이전에 전달되는 트래픽을 이용하기 때문에 분석 속도는 빠르지만, 암호화 트래픽 분석을 위해 충분한 사전 데이터가 수집되어야 한다.

VPN 환경에서 비밀 공유 스키마를 이용한 암호화 트래픽 분석 방법은 Shamir 비밀 공유 방식[5]을 이용한 방법으로, 메시지를 정해진 스키마에 맞게 n개로 분할하여 n개의 Proxy 서버로 전송한다. 메시지를 전달받은 Proxy 서버는 정해진 확률에 따라 메시지를 실제 목적지와 탐지 시스템으로 나누어 전송한다. 실제 목적지는 분할된 메시지를 복구하여 원래의 메시지를 수신하고, 탐지 시스템은 메시지를 복구하여 암호화된 트래픽을 분석한다. 트래픽의 내용을 직접 전달받을 수 있으므로 분석의 정확도가 높지만, 암호화 트래픽 분석을 위해 다수의 Proxy 서버와 클라이언트와 서버 사이에 공통된 비밀 공유 스키마의 공유가 필요하다.

본 논문에서 제안하는 방법은 서버와 클라이언트 사이에 전달되는 Handshake 메시지를 통해 세션키를 획득하여 암호화된 트래픽을 분석하는 방법으로, 기존 연구와 같은 사전 데이터나 추가적인 환경 구성없이 암호화된 트래픽을 검사할 수 있다.

3. SSL 보안 통신

SSL(Secure Socket Layer)은 전송계층 상에서 서버, 클라이언트에 대한 인증과 데이터 암호화를 제공하는 보안 프로토콜이다. SSL 통신은 서버와 클라이언트 사이에 세션을 생성한 뒤, 생성된 보안 채널을 통해 암호화 통신을 한다. 이때 암호화 통신에 필요한 세션키를 교환하기 위해 세션 생성 단계에서 SSL Handshake 과정을 거치게 된다. (그림 1) 은 SSL Handshake 과정을 나타낸다.



(그림 1) SSL Handshake 과정

SSL Handshake 과정에서 클라이언트와 서버는 Hello Message를 통해 랜덤 값 정보를 교환하며, 서버는 추가로 인증서를 클라이언트로 전달한다. Hello Message 교환 후, 클라이언트는 Secret 값을 서버 인증서로부터 추출한 서버의 공개키로 암호화하여 서버로 전달한다. 서버는 암호화된 메시지를 개인키로 복호화하여 Secret 값을 획득하고, 사전에 공유된 랜덤 값과 Secret 값을 이용하여 세션키를 생성한다.

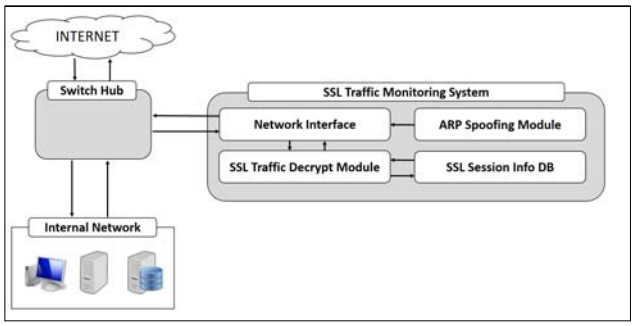
SSL Handshake 과정에서 서버의 공개키를 인증서를 통해 공유하는 방식은 통신의 제 3자가 세션키를 획득하는 것을 어렵게 만든다. 기존의 보안 장비의 경우 SSL 통신에 사용되는 세션키를 획득할 수 없으므로, 암호화 트래픽의 내용을 분석할 수 없다.

4. SSL 트래픽 분석 시스템

4.1 시스템 구조

본 논문에서 제안하는 SSL 트래픽 분석 시스템은 네트워크 인터페이스, ARP Spoofing 모듈, SSL 트래픽 복호화 모듈, SSL 세션 정보 DB로 구성된다. 분석 시스템의 동작은 다음의 순서로 진행한다.

ARP Spoofing 모듈은 네트워크 인터페이스를 통해 ARP Spoofing 메시지를 스위치 허브에 연결된 내부 네트워크로 전송하여 트래픽 흐름을 제어한다[6]. ARP Spoofing 메시지는 게이트웨이의 IP주소에 대한 물리 주소를 분석 시스템의 물리 주소로 변경하는 메시지로, 메시지를 수신한 호스트는 게이트웨이를 거쳐 내보내는 트래픽을 분석 시스템으로 전송하게 된다. 분석 시스템의 네트워크 인터페이스는 내부 호스트로부터 전달받은 트래픽 중 SSL 트래픽에 해당하는 패킷을 SSL 트래픽 복호화 모듈로 전달한다. SSL 트래픽 복호화 모듈은 전달받은 암호화 트래픽을 복호화하여 그 내용을 분석한다. SSL 트래픽 복호화에 필요한 세션 정보는 SSL 세션 정보 DB에 저장하여 관리한다. (그림 2) 는 논문에서 제안하는 시스템 구조를 나타낸다.



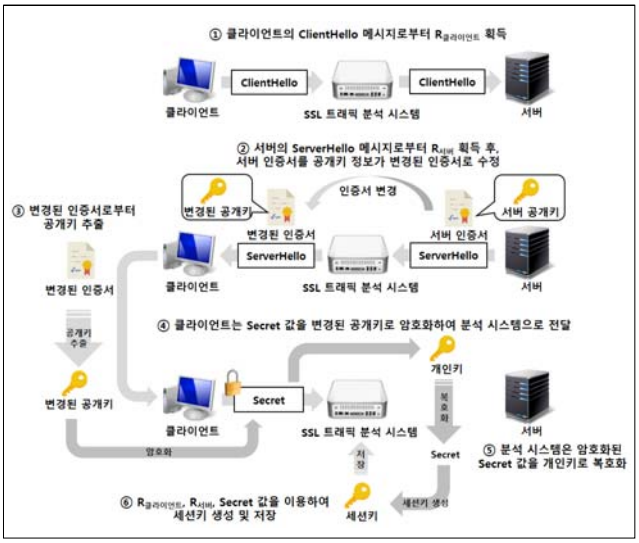
(그림 2) SSL 트래픽 분석 시스템 구조

4.2 SSL 세션키 획득

본 논문에서 제안하는 시스템은 SSL 트래픽을 복호화하기 위해 SSL Mitm(Man-in-the-middle)[7]을 이용하여 세션키를 획득한다. (그림 3)은 SSL 트래픽 분석 시스템에서 세션키를 획득하는 과정을 나타낸다.

SSL Handshake 과정에서 Client Hello, Server Hello 메시지에 포함된 랜덤 값 $R_{클라이언트}$, $R_{서버}$와 암호 알고리즘 정보를 획득한다. 그리고 Server Hello 메시지에 포함된 서버 인증서의 공개키 정보를 임의로 생성한 공개키 쌍의 공개키로 변경하여 클라이언트로 전송한다. 클라이언트는

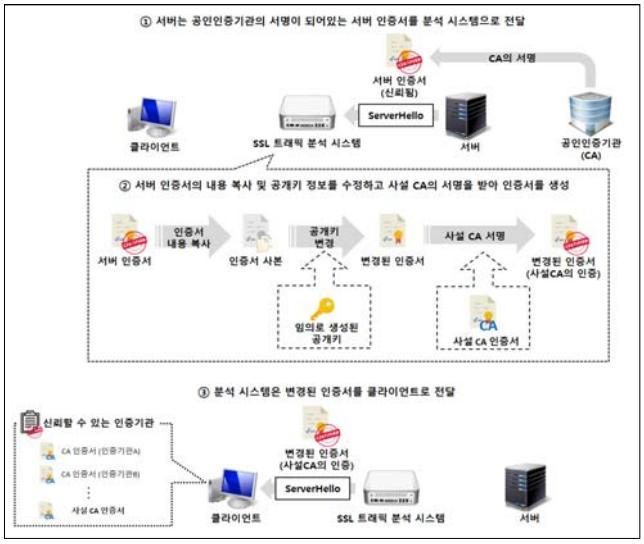
변경된 서버 인증서의 공개키를 추출하고, 추출된 공개키를 이용하여 Secret 값을 암호화하여 분석 시스템으로 전송한다. 이러한 과정은 SSL Handshake 과정에서 획득할 수 없는 서버 공개키 쌍 대신, 분석 시스템에서 생성한 공개키 쌍을 사용하여 세션키 생성에 필요한 Secret 값을 획득할 수 있게 한다. 암호화된 Secret 값을 전달받은 분석 시스템은 이전에 생성한 공개키 쌍의 개인키로 암호화된 Secret 값을 복호화하여 Secret 값을 획득한다. 분석 시스템은 SSL Handshake 과정에서 획득한 $R_{클라이언트}$, $R_{서버}$, Secret 값을 이용하여 세션키를 생성하고, 생성한 세션키와 암호 알고리즘 정보를 DB에 저장하여 암호화된 트래픽을 복호화할 때 사용한다.



(그림 3) SSL 세션키 획득 과정

4.3 서버 인증서 변경

서버 인증서 변경에 따른 클라이언트의 서버 인증서 검증 단계를 통과하기 위해 분석 시스템에서는 (그림 4)와 같은 과정으로 인증서를 생성하고 클라이언트로 전달한다.



(그림 4) 인증서 생성 및 전달 과정

서버로부터 Server Hello를 수신하면, 해당 메시지에서 서버 인증서 정보를 추출하여 인증서 사본을 생성한다. 생성된 인증서 사본의 공개키 정보는 탐지 시스템에서 생성한 공개키로 업데이트한다. 그리고 변경된 인증서에 대한 사설 CA 인증서의 서명을 추가하여 사설 CA의 인증을 받은 인증서를 생성한다.

사설 CA 인증서는 분석 시스템이 최초로 설치될 때 생성되며, 기업 내 모든 호스트에는 동일한 사설 CA 인증서가 배포된다. 배포된 사설 CA 인증서는 호스트의 신뢰할 수 있는 인증기관에 등록하여, 분석 시스템에서 변경한 인증서의 서버 인증서 검증 단계를 통과할 수 있도록 한다.

4.4 SSL 트래픽 복호화

SSL 트래픽을 복호화하기 위해 암호화된 패킷이 분석 시스템에 들어오면 해당 세션의 세션키와 암호 알고리즘을 SSL Session Info DB에서 검색한다. DB에 해당 세션의 정보가 존재하지 않는 경우, 분석 시스템을 거치지 않은 비정상적인 연결로 간주하고 해당 패킷을 버린다. DB에 해당 세션의 정보가 존재하는 경우, 저장된 세션키와 암호 알고리즘을 이용하여 암호화된 패킷을 복호화한다. 복호화된 패킷은 기존의 악성 행위 탐지 기술을 이용하여 악성 행위 유무를 판단하는 데 사용하거나, 정규식 패턴 매칭 기술을 이용하여 특정 패턴의 개인정보 유출을 탐지하는 데 사용할 수 있다. 복호화된 패킷은 기존 악성 행위 탐지 기술을 적용하여 악성 행위의 유무를 판단하거나, 정규식 패턴 매칭 기술을 이용한 개인정보 유출 탐지에 사용할 수 있다.

5. 결론

본 논문에서는 최근 증가하고 있는 암호화 트래픽을 이용한 악성 행위 탐지를 위해, SSL 암호화 트래픽을 복호화하여 분석할 수 있는 시스템을 제안하였다. 이러한 분석 시스템을 이용하면 기존의 암호화 트래픽 분석을 위해 필요한 사전 데이터나 추가적인 환경 구성없이 암호화된 트래픽을 검사할 수 있다. 제안하는 암호화 트래픽 검사 기술은 악성 행위 탐지뿐만 아니라 암호화 트래픽을 통해 내부정보 유출을 모니터링 할 수 있다. 또한, 분석 시스템의 전체 보안 수준의 저하 없이 암호화된 트래픽을 분석할 수 있다. 향후 연구로는 제안하는 분석 시스템을 이용하여 암호화된 악성 행위 및 내부정보 유출 탐지 기능을 구현하고, 이를 기업 네트워크 환경에 적용하여 분석 시스템의 성능을 검증할 것이다.

감사의 글

본 논문은 미래창조과학부 정보통신기술진흥센터 SW중심대학지원사업-SW중심대학 “무선 네트워크 보호를 위한 가상 게이트웨이 보안 기술 개발”의 지원으로 수행되

었음 (과제번호 R7115-16-1007).

참고문헌

[1] ESG “Network Encryption and its Impact on Enterprise Security” 2015.

[2] Gartner “Security Leaders Must Address Threats from Rising SSL Traffic” 2013.

[3] Husák, Martin, et al. "HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting," EURASIP Journal on Information Security, Vol.2016, No.30, 2016.

[4] Goh, Vik Tor, Jacob Zimmermann, and Mark Looi. "Detecting attacks in encrypted networks using secret-sharing schemes." International Journal of Cryptology Research 2.1, pp.89-99, 2010.

[5] Shamir, Adi. "How to share a secret." Communications of the ACM, Vol.22, pp.612-613, 1979

[6] Whalen, Sean. "An introduction to arp spoofing." Node99 [Online Document], 2001.

[7] Chomsiri, Thawatchai. "HTTPS Hacking protection." AINAW'07. 21st International Conference on. Vol. 1. IEEE, 2007.