공공 네트워크 환경에서 DNS 스푸핑 공격 탐지를 위한 통합 시스템

김건민[1], 이은성[1], 장현지[1], 이서준[1], 김경백[2]

1전남대학교 (학부생), 2전남대학교 인공지능융합학과 (교수)

Proposal for an Integrated System to Detect DNS Spoofing Attacks in Public Network Environment

Geon-Min Kim[1], Eun-Seong Lee[1], Hyeon-Ji Jang[1], Seo-Jun Lee[1], Kyung-Baek Kim[2]

1 Chonnam National University (Undergraduate Student)

2 Dept. of Artificial Intelligence Convergence, Chonnam National University (Professor)

요 약

본 논문은 공공 네트워크 환경, 특히 카페와 같은 공공 Wi-Fi에서의 DNS 스푸핑 공격을 효과적으로 방지하기 위한 통합 시스템을 제안한다. 제안된 시스템은 DNS 쿼리 모니터링을 Whitelist DB와의 통신과 결합하여 사용자가 접속한 도메인의 위변조 여부를 매칭하고, 이에 더해 Levenshtein 거리를 계산하여 유사한 URL을 이용하는 DNS 스푸핑 공격을 탐지하는 것을 목표로 한다.

I. 서론

DNS 스푸핑 공격[1]은 공격자가 DNS 응답을 조작하여 사용자를 악성 웹사이트로 유도하거나 네트워크를 침해하는 공격 기법이다. 이러한 공격은 특히 공공 Wi-Fi와 같은 개방된 네트워크 환경에서 심각한 보안 문제를 일으킬 수 있다. 본 논문에서는 DNS 쿼리 모니터링을 Whitelist[2] DB와의 통신과 결합하여 DNS 스푸핑 공격에 대응하는 시스템을 제안한다.

II. 시스템 설계

2.1 DNS 쿼리 모니터링

패킷 캡처 및 분석 도구(예: Wireshark)와 통계적 분석 기법을 활용하여 쿼리의 정상성 여부를 판단하고, 사용자가 접속하는 URL과 IP 정보를 모니터링한다.

2.2 Whitelist DB

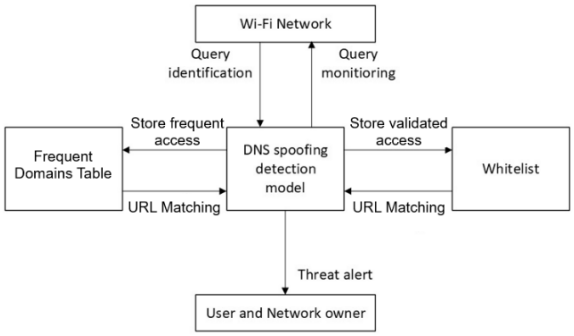
Whitelist DB는 사용자들이 자주 사용하는 승인된 도메인 주소 목록을 DB로 유지하며, 이를 통해 URL을 빠르게 대조할 수 있다. Whitelist DB는 중앙 DB 또는 분산 네트워크가 가능하며, 암호화된 프로토콜을 사용하여 보안성을 강화한다.

2.3 Frequent_domains table

사용자들이 자주 접속하는 도메인이 Whitelist에 존재하지 않는다면, 해당 도메인을 Frequent_domains 테이블에 저장한다. 이 테이블은 Whiteslist DB 내에 형성된다.

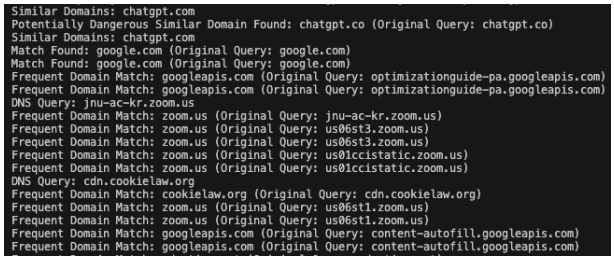
2.4 DNS 스푸핑 공격 탐지

유사한 URL을 사용하는 DNS 스푸핑 공격에 대응하기 위해 Levenshtein 거리[3]를 사용하여 두 도메인의 유사도를 계산한다. threshold 값으로 2 이하의 Levenshtein 거리(두 문자열 간의 최소 편집 거리)를 가진 도메인은 유사한 것으로 간주하여, 사용자에게 즉각적으로 경고한다.



(그림 1) DNS 스푸핑 공격 탐지를 위한 시스템 제안

III. 구축 결과



(그림 2) 구축한 시스템의 DNS query monitoring 결과

Case	Output
기본적인 모니터링된 DNS query	DNS Query:
모니터링된 DNS query가 Whitelist DB에 존재하는 경우	Match Found:
Whitelist DB에는 존재하지 않으나 사람들이 최근에 자주 접속한 도메인의 경우	Frequent Domain Match:
DNS Query가 Whitelist DB의 주소와 유사하나 다른 경우	Potentially Dangerous Similiar Domain Found:

(표 1) DNS query monitoring 결과 설명

Whitelist에는 없으나 이용자들이 자주 모니터링 되어 안전하다 판단되는 URL은 Frequent_domains 테이블에 업데이트 된다. 해당 URL이 이미 Frequent_domains 테이블에 존재하면 count를 증가시키고, 존재하지 않으면 새로 추가한다. 위의 (그림 2)에서 DNS Query: jnu-ac-kr.zoom.us의 경우 처음 발견된 DNS 쿼리이고, 해당 URL이 다시 나타나니 Frequent Domain Match:로 전환되어 결과가 출력되는 것을 확인할 수 있다.

또한, (그림 2)에서 chatgpt.com과 유사한 URL을 사용하는 chatgpt.co의 접속에 대해서는 즉각적으로 Potentially Dangerous Similar Domain Found:로 경고를 띄우는 것을 확인할 수 있다.

IV. 결론

본 논문에서는 공공 네트워크 환경에서 DNS 스푸핑 공격을 효과적으로 방지하기 위한 통합 시스템을 제안하였다. 제안된 시스템은 공공 Wi-Fi와 같은 불특정 다수가 이용하는 네트워크 환경에서의 보안성을 향상시키는 데 기여할 수 있다. 향후 연구에서는 Whitelist DB의 신뢰성 유지를 위해 보안성을 강화할 수 있는 기술적 개선 방안이 요구되며, 특히 부적절한 URL이 Frequent_domains 테이블에 추가되지 않도록 하는 URL 필터링 기준에 대한 체계적인 연구가 필요하다.

ACKNOWLEDGEMET

본 연구는 한국인터넷진흥원(KISA)-정보보안특성 화대학 지원사업의 지원을 받아 수행된 연구임. 본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업의 연구결과입니다.

[참고문헌]

[1] A. Jony, M. N. Islam and I. H. Sarker, "Unveiling DNS Spoofing Vulnerabilities: An Ethical Examination Within Local Area Networks," 2023 26th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh, 2023, pp. 1-6

[2]K. Hasegawa, D. Kondo and H. Tode, "FQDN-Based Whitelist Filter on a DNS Cache Server Against the DNS Water Torture Attack," 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 2021, pp. 628-632

[3]Sugiarto, I. G. S. M. Diyasa and I. N. Diana, "Levenshtein Distance Algorithm Analysis on Enrollment and Disposition of Letters Application," 2020 6th Information Technology International Seminar (ITIS), Surabaya, Indonesia, 2020, pp. 198-202