Authentication-Results 헤더 확장 및 ARC 프로토콜을 통한 SMTP 다운그레이드 공격 방어 기법

남재호, 김현수, 권태경
서울대학교

jhnam@mmlab.snu.ac.kr, hskim@mmlab.snu.ac.kr, tkkwon@snu.ac.kr

Mitigating SMTP Downgrade Attacks through Extension of Authentication-Results Header and ARC Protocol

Jaeho Nam, Hyunsoo Kim, Ted “Taekyoung” Kwon
Seoul National Univ.

요 약

이메일 시스템의 핵심에 있는 SMTP 는 평문 기반으로 설계되어 STARTTLS 다운그레이드 등의 취약점이 존재한다. 이를 보완하기 위해 DANE, MTA-STS 등의 프로토콜이 제안되었으나 복잡한 운영 구조로 인해 사용률은 저조한 수준에 머물러 있다. 본 논문은 Authentication-Results 헤더를 확장해 SMTP 트랜잭션 내의 STARTTLS 관련 상호작용 정보를 기록하고 이를 ARC 프로토콜로 보호하여 다운그레이드 공격을 탐지하는 기법을 제안한다. 또한, STARTTLS 에서 범위를 확장하여 SMTP 명령 시퀀스의 무결성을 검증할 수 있는 방법을 추가로 제안한다. 본 기법은 별도 인프라 없이 적용 가능하여 도입 장벽이 낮고, 경량화되고 높은 확장성을 갖춘 이메일 보안 프로토콜을 새롭게 제시하였다는 점에서 의의가 있다.

Ⅰ. 서론

이메일은 오늘날 개인 간의 연락을 비롯하여 기업 업무, 행정 등 모든 영역에서 필수적인 디지털 커뮤니케이션 수단으로 사용되고 있다. 따라서 이메일 시스템의 신뢰성과 보안은 디지털 환경의 안전과 관련된 중요한 요소라 할 수 있다. 그러나 이메일 시스템의 근간을 이루는 SMTP(Simple Mail Transfer Protocol)는 처음 표준화될 당시 보안 위협을 고려하지 않은 채 기본적으로 평문으로 동작하도록 설계되었고 이는 오늘날까지도 이메일 보안 측면에서 심각한 문제를 초래하고 있다. 대표적으로 발신자 이메일 주소를 위조하여 합법적인 사용자로 가장하는 이메일 스푸핑 공격, 민감한 이메일 본문이 가로채이거나 변조될 위험으로 이어질 수 있는 STARTTLS 다운그레이드 공격 등이 있다. 이 중 STARTTLS 다운그레이드 공격을 방어하기 위해 DANE(DNS-Based Authentication of Named Entities), MTA-STS(Mail Transfer Agent Strict Transport Security)와 같은 보안 프로토콜이 제안되었다. DANE 은 DNSSEC(Domain Name System Security Extensions)을 기반으로 TLS(Transport Layer Security) 인증서를 검증하는 방식이며, MTA-STS 는 수신 메일 서버의 TLS 요구 정책을 HTTPS(Hypertext Transfer Protocol Secure) 웹 서버를 통해 게시함으로써 보안을 강화한다.

그러나 이러한 프로토콜들의 실질적인 사용률은 여전히 낮은 수준에 머물러 있다.[1] DANE 의 경우 DNSSEC 세팅이 필수적인데 복잡한 운영 절차와 높은 관리 비용으로 인해 도입이 활발히 이루어지지 않고 있다. MTA-STS 또한 정책을 별도의 HTTPS 웹 서버를 통해 호스팅해야 하는 부담이 있으며, DNSSEC 없이 운영되는 환경에서는 여전히 DNS 기반 위조에 취약하다. 즉, 두 프로토콜 모두 외부 채널(DNSSEC, HTTPS)을 활용해 인증 정보를 강화하는 구조적인 특성을 가지는데, 이러한 채널들을 간단히 구성하면서도 안전하게 운영하는 두 가지 목적을 동시에 달성하기는 쉽지 않다. 이에 따라 향후 해당 프로토콜들의 도입률이 크게 증가할 것으로 기대하기는 어렵다.

본 논문에서는 외부 채널을 활용하는 기존 방식 대신, SMTP 트랜잭션 자체의 기능과 ARC(Authenticated Received Chain)[5] 프로토콜을 이용하여 평문 전송 구간의 무결성을 검증할 수 있는 방법을 제안한다. 이 방식은 별도의 인프라 구성이 필요 없다는 점에서 실제 도입 시의 운영 부담을 크게 줄일 수 있으며, 이미 표준화된 이메일 인증 프로토콜을 활용함으로써 높은 적용 가능성도 기대할 수 있다.

Ⅱ. 본론

SMTP 는 기본적으로 평문 기반의 프로토콜이며, TLS 를 통한 암호화는 확장 SMTP(ESMTP)의 STARTTLS 확장을 통해 선택적으로 제공된다. SMTP 서버는 EHLO 명령에 대한 응답에서 STARTTLS 확장을 지원한다고 명시할 수 있으며, 클라이언트는 이를 확인한 후 STARTTLS 명령을 사용해 기존 평문 연결을 TLS 연결로 업그레이드 할 수 있다. STARTTLS 다운그레이드 공격은 중간자 공격(Man-in-the-Middle)의 일종으로, SMTP 트랜잭션 중 클라이언트와 서버 간에 교환되는 STARTTLS 관련 메시지를 변조하거나 제거하여 평문 통신을 강제로 유도하는 능동적(active) 공격에 해당한다. 그림 1 에서 확인할 수 있듯이 서버가 클라이언트에게 보내는 EHLO 응답 내의 STARTTLS 확장 문자열을 변조하거나 클라이언트의 STARTTLS 명령을 중간에서 제거하는 방식이 있다.[2]

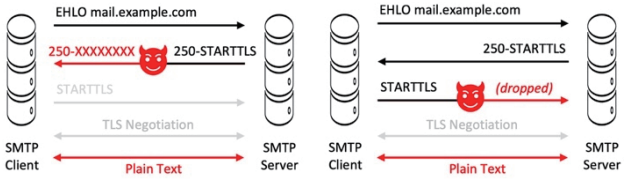

그림 1. 2 가지 STARTTLS 다운그레이드 공격 타입

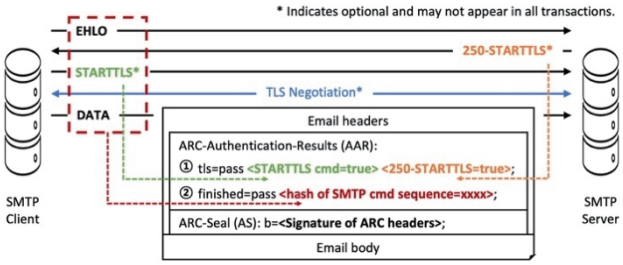

그림 2. STARTTLS 상호작용 및 SMTP 명령 시퀀스를 무결성 있게 기록하기 위한 ARC 프로토콜 기반 메시지 구조

이와 같은 위협 모델에 대응하기 위해, 본 논문에서는 클라이언트가 STARTTLS 확장을 수신했는지 여부와, 수신한 경우 STARTTLS 명령을 통해 TLS 연결을 시도했는지를 이메일 헤더에 기록하여 서버로 전달하는 방식을 제안한다. 서버는 해당 정보를 바탕으로 다운그레이드 공격 여부를 판단하고 적절한 대응을 수행할 수 있다. EHLO 명령 및 그에 대한 응답, 그리고 STARTTLS 명령의 전송 여부는 모두 이메일 메시지를 전송하기 위한 DATA 명령 이전에 발생하는 이벤트이므로, 이와 관련된 정보를 이메일 헤더에 포함시키는 것이 가능하다. TLS 연결을 지원하는 서버의 관점에서는 이메일 메시지가 평문으로 전송될 때 공격 여부를 다음과 같이 판단할 수 있다:

1) 클라이언트가 STARTTLS 확장을 수신하지 못한 경우: EHLO 응답이 중간자에 의해 변조된 것으로 간주할 수 있으며, 이는 다운그레이드 공격으로 판단한다.

2) 클라이언트가 STARTTLS 확장을 수신하고 명령을 시도했으나, 서버가 해당 명령을 수신하지 못한 경우: STARTTLS 명령이 중간자 공격에 의해 삭제된 것으로 판단한다.

3) 클라이언트가 STARTTLS 확장을 수신했지만 TLS 를 지원하지 않아 평문 전송을 수행한 경우: 이는 클라이언트의 기능적 제약에 의한 것으로, 공격으로 간주하지 않는다.

클라이언트의 TLS 관련 처리 결과는 RFC 8601 에 정의된 Authentication-Results 헤더[3]를 통해 서버로 전송할 수 있다. 위 헤더는 기본적으로는 다양한 이메일 인증 프로토콜(SPF, DKIM, DMARC 등)의 평가 결과를 기록하기 위한 용도로 사용되지만, 사용자 정의(custom) 평가 항목의 추가도 허용된다. 그러나 능동적 공격자가 개입하여 이메일이 평문으로 전송될 경우 이메일 헤더 또한 공격자의 조작 대상이 될 수 있으며, 이로 인해 클라이언트의 TLS 처리 결과가 수신 서버로 안전하게 전달되지 않을 수 있다. 이러한 문제를 해결하기 위해 본 논문에서는 이메일 스푸핑 공격 방어에 활용되는 ARC 프로토콜을 사용하여 추가적으로 헤더의 무결성을 보장하는 방안을 제안한다. ARC 에서는 Authentication-Results 와 동일한 역할을 수행하는 ARC-Authentication-Results(AAR) 헤더를 정의하고 있으며, 이는 ARC-Seal(AS) 헤더를 통해 서명되어 무결성이 보호된다. 따라서 클라이언트가 ARC 프로토콜을 지원하는 경우, STARTTLS 관련 상호작용 정보를 그림 2 의 ①과 같이 변조 방지된 형태로 수신 서버로 안전하게 전달할 수 있다.

그러나 능동적 공격자는 STARTTLS 외에도 평문으로 전송되는 SMTP 명령 구간에 개입하여 다양한 방식으로 공격을 수행할 수 있으며, 이러한 공격은 앞서 소개한 기법으로는 탐지할 수 없다. 특히, REQUIRETLS[4]와 같이 SMTP 트랜잭션 보안을 강화하기 위한 새로운 확장 프로토콜이 도입될 경우, 이들에 대한 방어가 불가능하다. 이를 해결하기 위해 TLS 연결 수립 이전에 송수신되는 SMTP 명령 시퀀스의 무결성을 검증할 수 있는 구조를 추가적으로 제안한다. 제안하는 방식은 클라이언트가 TLS 연결 이전에 송수신한 모든 SMTP 명령(EHLO, STARTTLS, MAIL FROM 등)을 순서대로 기록한 후, 해당 시퀀스에 대한 해시 값을 계산하고 그림 2 의 ②와 같이 AAR 헤더를 통해 수신 서버에 전달하는 것이다. 이 해시는 ARC 프로토콜의 AS 헤더를 통해 서명되므로 중간자가 이를 변조하는 것은 불가능하며, 수신 서버는 자체적으로 기록한 SMTP 명령 흐름과 AAR 헤더로 전달받은 해시 값을 비교함으로써, 양측이 동일한 SMTP 컨텍스트를 공유하고 있는지를 검증할 수 있다.

본 논문에서 제안한 방식은 실제 환경에서의 적용을 고려할 때 몇 가지 고려할 점이 존재한다. 첫째로, 능동적 공격자가 ARC 관련 헤더 자체를 전송 중에 제거(drop)할 가능성이 존재한다. 그럼에도 불구하고 ARC 헤더의 부재는 수신 서버 입장에서 하나의 이상 징후로 작용할 수 있으며, 수신 메일 서버가 보안 정책을 강화하는 방향으로 대응한다면 기존 대비 공격 가능성은 실질적으로 낮아진다. 둘째로, SMTP 에는 DATA 명령이 실행된 이후 메시지 전송을 취소(abort)할 수 있는 메커니즘이 존재하지 않는다. 따라서 공격자가 평문 전송을 유도할 경우 이메일 본문은 여전히 감청될 수 있으며 사후 대응만 가능하다. 그러나 공격 탐지 이후 수신 서버는 특정 발신자나 경로에 대해 보다 강화된 보안 정책을 적용함으로써 지속적인 대응이 가능하다. 또한, 본 기법은 운영 부담을 줄이는 이점을 가지므로 인프라 구성에 어려움을 겪는 이메일 서비스 제공 업체에게 하나의 대안이 될 수 있다.

Ⅲ. 결론

본 논문에서는 Authentication-Results 헤더에 사용자 정의 메소드를 추가하여 SMTP 명령 상호작용에 대한 결과를 기록하고 이를 ARC 의 서명 기능으로 보호받음을 통해 SMTP 트랜잭션 중 발생할 수 있는 다운그레이드 공격을 효과적으로 감지하는 새로운 기법을 제안하였다. 이러한 방식은 별도의 외부 채널을 요구하지 않기 때문에 기존 낮은 사용률을 가지고 있는 DANE 이나 MTA-STS 프로토콜과 비교하여 도입 장벽과 운영 복잡성을 낮출 수 있는 이점이 있다. 동시에 ARC 프로토콜을 기반으로 동작하기 때문에 이메일 인증 프로토콜과의 자연스러운 통합이 가능하며, 하나의 프로토콜 안에서 두 가지 보안 목표를 동시에 달성할 수 있게 된다. 본 기법은 향후 보다 경량화되고 통합적인 이메일 보안 프로토콜의 발전 방향을 제시한다는 점에서도 중요한 의의를 가진다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00220985).

참 고 문 헌

[1] B. Blechschmidt and B. Stock, “Extended Hell(o): A Comprehensive {Large-Scale} Study on Email Confidentiality and Integrity Mechanisms in the Wild,” presented at the 32nd USENIX Security Symposium (USENIX Security 23). 2023, pp. 4895- 4912.

[2] D. Poddebniak, F. Ising, H. Böck, and S. Schinzel, “Why {TLS} is better without {STARTTLS}: A Security Analysis of {STARTTLS} in the Email Context,” presented at the 30th USENIX Security Symposium (USENIX Security 21). 2021, pp. 4365- 4382.

[3] M. Kucherawy, “Message Header Field for Indicating Message Authentication Status,” Internet Engineering Task Force, Request for Comments RFC 8601, May 2019.

[4] J. Fenton, “SMTP Require TLS Option,” Internet Engineering Task Force, Request for Comments RFC 8689, Nov. 2019.

[5] K. Anderson, et al. “The authenticated received chain (ARC) protocol.” Internet Engineering Task Force, Request for Comments RFC 8617, Jul 2019.