해킹메일 대응을 위한 기술 표준 분석

변예은*
*한국원자력통제기술원
hibye@kinac.re.kr

Analysis of Technical Standards for Hacking Mail

Ye-Eun Byun*
*Korea Institute of Nuclear Nonproliferation and Control

요 약

해킹메일로 인한 피해는 꾸준히 발생하고 있으며, 최근에는 정부나 공공기관을 사칭하는 메일로 인한 피해 사례가 증가하고 있어 정부에서는 사칭메일을 대응하기 위한 기술을 적용하도록 요구하고 있다. 2017년부터 한국인터넷진흥원에서는 이메일 주소를 사칭하는 메일을 차단하기 위해서는 SPF(Sender Policy Framework) 기술을 적용해야 한다고 밝혔으며, 2019년에 정부에서는 SPF 뿐만 아니라 DKIM(Domain Keys Identified Mail)과 DMARC(Domain-based Message Authentication, Reporting, and Conformance)까지 적용을 확대할 것을 요구하고 있다. 이에, 본 논문에서는 해킹메일 대응을 위해 적용하고 있는 세 가지 기술의 기술 표준을 분석함으로써 해당 기술을 적용하여 나가기 위한 발판을 마련하고자 한다.

1. 서론

최근에 해킹메일로 인한 피해가 꾸준히 증가하고 있으며, 그 중에서도 정부나 공공기관을 사칭한 메일로 인한 피해가 증가하고 있어 정부에서는 이러한 사칭메일을 대응하기 위하여 각 기관에서 보안 기술을 적용하도록 요구하고 있다. 2017년부터 이미 한국인터넷진흥원에서는 이메일 주소를 사칭하는 메일을 차단하기 위해서 이메일 발신 서버의 진위 여부를 판단하는 SPF(Sender Policy Framework) 기술을 적용해야 한다고 밝혔으며, 2019년부터 정부에서는 SPF 뿐만 아니라 전자서명 방식의 DKIM (Domain Keys Identified Mail)을 통해 발신자가 발송한 메일의 위변조 여부를 확인할 수 있는 기술을 적용하여야 한다고 밝힌 바 있다. 또한 SPF와 DKIM을 모두 적용한 DMARC(Domain-based Message Authentication, Reporting, and Conformance)까지 적용을 확대할 것을 요구하고 있다. 이에, 본 논문에서는 최근 이슈가 되고 있는 해킹메일 대응을 위하여 적용하고 있는 기술인 SPF, DKIM, DMARC의 기술이 어떠한 표준 문서와 체계에 의해 마련되었는지를 살펴보기 위해 해당 기술 표준에 대해 분석하여 보고자 한다.

2. 본론

우선, 기술 표준 관련 문서들의 체계를 살펴보기 위하여 먼저 기술 표준을 만드는 협회와 기술 표준 문서 체계에 대해 살펴보고, 각 기술에 관련된 기술 표준에 대해 살펴보고자 한다.

2.1 IETF RFC

국제인터넷표준화기구(Internet Engineering Task Force, IETF)에서는 인터넷 관련 기술 표준을 만드는데, 이 과정에서 생산되는 문서를 RFC(Request For Commands)라 하고 이는 인터넷에서 기술을 구현할 때 필요한 절차 등을 제공하는 문서로 활용된다.

2.2 SPF 관련 기술 표준 분석

SPF(Sender Policy Framework)와 관련한 RFC 문서를 분석한 결과는 다음과 같다. SPF에 대해서 주로 다루고 있는 문서는 RFC 7208로, 이는 RFC 4408을 검토하고 개정하여 표준(Standard)으로 정해진 문서이다.[1] 이전 버전으로 볼 수 있는 RFC 4408은 실험적인(Experimental) 문서로 분류되었으며, 이는 검증되거나 범용적으로 활용되기 전 단계의 문서로서의 성격을 띈다.[2] 또한, RFC 6686은 정보 전달(Informational)의 문서로, 해당 문서에서

언급하고 있는 두 가지 메일 인증 프로토콜 중 하나인 Sender ID 프로토콜은 RFC 4406(Sender ID : Authenticating E-Mail)에서 제안하고 있는 실험적인(Experimental) 것으로, SMTP 서버가 수신된 메일의 주소가 해당 메일 주소의 DNS의 검증을 받았는지 여부를 판별할 수 있는 기술에 대해 설명한다.[3]

<표 1> SPF 관련 기술 표준

문서번호	제목	주요 내용
RFC 4408 (‘06.04)	Sender Policy Framework(SPF) for Authorizing Use of Domains in E-Mail, Version 1	- 보내는 사람이 도메인 네임을 사용할 수 있는지를 검증하고, 받는 사람도 그 검증을 확인하는 SPF 프로토콜에 대해 설명
RFC 7208 (‘14.04)		- ADministrative Management Domains(ADMDs)가 상기 내용을 검증하는 프로토콜에 대해 설명
RFC 6652[4] (‘12.06)	SPF Authentication Failure Reporting Using the Abuse Reporting Format	- 메시지 인증 실패 시, 상세하게 보고할 수 있는 방식에 대해 설명 - 본 문서를 통해 RFC 4408 업데이트. 표준(Standard)
RFC 6686 (‘12.07)	Resolution of the SPF and Sender ID Experiments	- SPF와 Sender ID 두 가지의 메일 인증 프로토콜의 차이점 등에 대해 설명

2.3 DKIM 관련 기술 표준 분석

다음으로 DKIM(Domain Keys Identified Mail)와 관련한 RFC 문서를 분석한 결과는 다음과 같다. DKIM 기술을 설명할 때 일반적인 표준 기술은 RFC 4871이며, 이 문서는 도메인 별로 이메일에 디지털 서명을 하기 위한 프레임 워크를 정의한 RFC 4870을 업데이트 하여 작성되었다.[5]

<표 2> DKMI 관련 기술 표준

문서번호	제목	주요 내용
RFC 4871 (‘07.05)	Domain Keys Identified Mail (DKIM) Signatures	- 공개키 암호화와 키 서버 기술을 사용하는 도메인 수준의 인증 프레임워크 설명
RFC 5672 (‘09.08)	RFC 4871 Domain Keys Identified Mail (DKIM) Signitures -- Update	- RFC 4871을 업데이트 - 제안된 기술(Proposed Standard)
RFC 6376[6] (‘11.09)	DomainKeys Identified Mail (DKIM) Signatures	- DKIM 서명을 유지하는 방식을 통해 메일이 전송되는 방식에 대해 설명 - RFC 4871을 업데이트하여 작성된 표준(Standard)
RFC 8301[7] (‘18.01)	Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail(DKIM)	- DKIM이 설계되었을 때, 포함된 암호 알고지름과 키 크기 요구사항에 대한 부분을 수정 - RFC 6376을 업데이트
RFC 8463[8] {‘18.09}	A new Cryptographic Sighnature Method for DomainKeys Identified Mail(DKIM)	- RFC 6376을 업데이트

또한, RFC 4871은 RFC 5672를 통해 업데이트 되는데, 문서를 살펴보면 RFC 4871에서 언급한 내용의 한 문장씩을 수정하기도 하고 SDID(Signing Domain Identifier)라는 새로운 개념을 도입하기도 한다.[9]

2.4 DMARC 관련 기술 표준 분석

마지막으로 DMARC(Domain-based Message Authentication, Reporting, and Conformance)와 관련한 RFC 문서를 분석한 결과는 다음과 같다.

<표 3> DMARC 관련 기술 표준

문서번호	제목	주요 내용
RFC 7489 (‘15.03)	Domain-based Message Authentication, Reporting, and Conformance	- 정보 전달Informational)의 문서

	(DMARC)	
RFC 7960 (‘16.09)	Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows	- 정보 전달Informational)의 문서

RFC 7489에서는 메일 발신자가 도메인 수준의 정책 및 기본 설정을 처리할 수 있는 메커니즘인 DMARC에 대해 설명을 하고 있다.[10] 또한, RFC 7960에서는 DMARC 메커니즘을 사용하였을 때, 메시지가 발신자의 도메인에서 수신자에게 직접 전달되지 않는 경우 발생할 수 있는 상호 운영성의 문제를 ‘간접 이메일 흐름’이라 정의하고 이를 해결하기 위한 방안을 제시하고 있다.[11]

3. 결론

최근 메일 수신자가 관심을 가지는 내용의 제목으로 클릭을 유도하는 피싱 메일이나 특정 집단을 타겟으로 하여 정부기관 등을 사칭하는 해킹 메일 등 다양한 기법을 통해 해킹 메일이 사용자들에게 유포되고 있다. 이에, 정부에서도 각 기관에서의 피해를 방지하기 위해 SPF・DKIM・DMARC의 기술을 적용할 것을 요구하고 있고, 보안 업체에서도 갈수록 발전하고 있는 공격 기법에 대응하기 위한 제품들을 출시하고 있다. 본 논문에서는 이러한 사회적인 환경에서 요구하고 있는 보안 기술들의 체계와 해당 기술들의 표준 문서에 대해 살펴보았다. 보안 기술을 적용하기 위해 해당 기술이 제안되거나 적용되고 있는 문서의 흐름을 파악하는 것은 기술 도입 전 이해를 돕기 위한 발판이 되었으며, 이를 통해 보다 폭 넓은 기술적인 이해를 할 수 있을 것이라 기대해본다. 물론 다양한 보안 기술을 적용함으로써 기관 내 보안대책을 강화하는 것도 중요하지만 무엇보다 중요한 것은 의심되는 메일은 열어보지 않고, 기본적인 보안 수칙을 준수하는 사용자들의 보안 의식이 가장 중요할 것이다.

참고문헌

[1] S. Kitterman, “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1”, 2014

[2] M. Wong, W. Schlitt, “Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1”, 2006

[3] M. Kucherawy, “Resolution of the Sender Policy Framework (SPF) and Sender ID Experiments”, 2012

[4] S. Kitterman, “Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format”, 2012

[5] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures”, 2007

[6] D. Crocker, Ed., T. Hansen, Ed., M. Kucherawy, Ed., “DomainKeys Identified Mail (DKIM) Signatures”, 2011

[7] S. Kitterman, “Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)”, 2018

[8] J. Levine, “A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)”, 2018

[9] D. Crocker, Ed., “RFC 4871 DomainKeys Identified Mail (DKIM) Signatures – Update”, 2009

[10] M. Kucherawy, Ed., E. Zwicky, Ed., “Domain-based Message Authentication, Reporting, and Conformance (DMARC)”, 2015

[11] F. Martin, Ed., E. Lear, Ed., T. Draegen. Ed., E. Zwicky, Ed., K. Andersen, Ed., “Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows”, 2016