아마존 S3를 통해 본 클라우드 컴퓨팅 환경에서의 스토리지 보안

신승목*, 김광조*

*정보통신공학과, KAIST

Considering storage security for Cloud computing environment in the case study of S3

Sung-Mok Shin*, Kwangjo Kim*

*Department of Information and Communications Engineering, KAIST

요 약

최근 클라우드 컴퓨팅이 많은 각광을 받으면서 아마존 EC2 & S3, 구글 App Engine, 마이크로소프트 애저(Azure)등의 서비스들이 주목받고 있다. 클라우드 컴퓨팅 벤더들은 대량의 서비스를 기본으로 하여 보다 많은 고객들의 서비스를 자신의 클라우드에 유치함으로써 수익 증대와 함께 자원 활용률을 높여 규모의 경제를 달성하려고 하고 있다. 하지만 선행되어야 할 것은 신뢰성 있고 안정성 있는 서비스를 제공하려는 벤더들의 연구 노력이다.

본 논문에서는 업계의 de facto 표준으로 자리 잡고 있는 아마존 AWS(Amazon Web Service)에 대해 알아보고 AWS의 스토리지 서비스인 S3(Simple Storage Service)에 대한 보안 위협에 대해 알아본다. 또한 S3의 구조적인 특성으로 인해 서비스 거부 공격(Denial of Service)과 중간자 공격 (Man-in-the-Middle-attack) 공격에 취약하다는 점을 지적한다. 이러한 공격에 의해 S3는 서비스를 더 이상 제공하지 못하거나, 악의적인 HTTP 쿼리를 허용하게 될 수 있다.

I. 서론

클라우드 컴퓨팅은 IT 시스템을 기업이 자체적으로 구축하지 않고, 신뢰할 수 있는 제 3자의 인프라에 구현된 서비스에 액세스하는 컴퓨팅 방식이다. [2, 8]. 클라우드 컴퓨팅은 확장 가능한 애플리케이션을 만들고 제공하는 방법에 있어서 패러다임의 변화를 가져오고 있다. 과거에는 기업에서 시간과 리소스를 투자하여 인프라를 구축하였으며, 이 인프라가 바로 기업 경쟁력이 되었다. 하지만 이러한 시간과 리소스는 프로젝트의 성공 여부에 따라 비용을 지불하려는 회사나 사용자가 나타나지 않는 한 결국 폐기되고 만다.

하지만 클라우드 컴퓨팅에서는 잉여 컴퓨팅 성능을 고객에게 판매하여 위와 같은 단점을 제거한다. 클라우드 컴퓨팅으로의 전환을 통해 다음과 같은 장점을 얻을 수 있다 [7].

- 서버 관리를 위한 인력 비용 절감
- 사용되지 않는 많은 양의 컴퓨팅 자원에 대한 구입비용 절감
- 서버 운용에 드는 에너지 비용 절감

클라우드 컴퓨팅의 주요 성공 사례로는 'SmugMug', '37Signal', 'New York Times'등이 있다. SmugMug는 500TB이상의 데이터를 아마존 웹 서비스에 저장하는 온라인 포토 스토리지 애플리케이션이며, 37Signal은 온라인 프로젝트 관리 소프트웨어인 'Basecamp'의 제작업체로 S3(Simple Storage Service)를 사용하여 저장장치 요구를 해결하고 있다. New York Times는 용량이 수 TB에 달하는 아카이브 데이터를 수백 개의 EC2 인스턴스를 사용하여 36시간 이내에 디지털화한 이력이 있다.

하지만 이러한 장점과 높은 관심에도 불구하고 아직 클라우드 컴퓨팅이 본격적으로 도입되고 있지 않은 이유는 아직 이 기술이 사용자에게 높은 신뢰감을 주지 못하고 있기 때문이다

[9]. 클라우드 컴퓨팅이 IT업계의 패러다임을 바꾸는 기술이 되기 위해서는 현재 이에 관련해 대두되고 있는 문제점들을 효과적으로 해결할 수 있는 방법이 제시되어야 한다 [5, 7].

아마존 웹 서비스 AWS(Amazon Web Service)에서 스토리지 서비스를 제공하고 있는 S3는 버킷(Bucket)과 오브젝트(Object) 단위로 구성된 대용량 스토리지 서비스이고, HTTP 쿼리를 통해 유연한 데이터 액세스 및 수정 기능을 제공한다. 하지만 S3는 사용자의 데이터 기밀성을 만족시켜주지 못하고 서비스 거부(Denial of Service) 공격, 중간자 공격(Man-in-the-Middle attack)에 취약할 수 있다.

본 논문에서는 아마존 AWS에 대해 알아보고, 그 중 스토리지 서비스를 제공하는 S3에 대한 보안 위협에 살펴본다. 2장에서는 AWS와 S3의 구조에 대해 알아보고, 3장에서는 클라우드 컴퓨팅의 보안 모델에 관해 알아보고 공격을 위한 기본 가정에 대해 기술한다. 4장에서는 S3에 대해 시도 가능한 공격에 대해 알아보고 5장에서 결론을 내린다.

II. 관련연구

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅은 외부 환경에서 서비스로 제공되는 확장 가능한 컴퓨팅 리소스를 사용량에 따라 요금을 지불하는 식의 컴퓨팅 방식이라 정의할 수 있다. 시간과 장소에 제약을 받지 않고 인터넷을 통해 “클라우드”에 액세스 하여 필요한 리소스만 요청하여 사용할 수 있다. 그러면서도 화면 뒤의 클라우드에 있는 리소스의 유지 관리에 신경을 쓰지 않아도 된다. 또한 클라우드는 애플리케이션의 요구에 대한 높은 가용성과 빠른 응답성을 지원한다.

2.2 국내외 연구 현황

국내외에서 많은 벤더 및 연구 단체들이 클라우드 컴퓨팅에 관한 연구 및 개발을 진행하고 있다. 다음은 클라우드 컴퓨팅 개발 및 연구에 주도적인 역할을 하고 있는 벤더 및 단체들이다.

○ 아마존(Amazon)

아마존은 최초로 대중용 클라우드 컴퓨팅 서비스를 제공함으로써 대중에게 클라우드 컴퓨팅의 인지도를 향상 시켰다 [10]. 이는 기존에 이미 검증된 네트워크 인프라, 데이터센터가 있기에 가능한 일이었다. 또한 아마존은 "Pay-As-you-Go"라는 슬로건 아래 서비스를 사용한 만큼만 지불한다는 과금 체계를 정착시켰다.

○ 마이크로소프트(Microsoft)

마이크로소프트는 클라우드 컴퓨팅을 위한 윈도우인 ‘윈도우 애저(Windows Azure)’와 이의 기반이 되는 서비스 플랫폼인 ‘애저 서비스플랫폼’을 발표하고 클라우드 컴퓨팅 개발을 강화하고 있다 [11].

○ 구글(Google)

구글은 현재 기업 트렌드가 클라우드 컴퓨팅이라고 전망하고 기존에 보유한 여러 클라이언트 서비스를 하나로 묶을 수 있는 AppEngine 플랫폼에 개발 및 연구 노력을 기울이고 있다 [12].

○ 한국 클라우드컴퓨팅연구조합

국내에서는 한국 클라우드컴퓨팅연구조합이 4월에 개소하여 산학연간 긴밀한 협조를 통해 글로벌 기술 경쟁력 확보에 나서고 있다.

○ 한국정보보호학회

한국정보보호학회 산하에 클라우드 컴퓨팅 보안 기술 연구회가 운영되고 있으며 현재 클라우드 컴퓨팅의 보안 취약점과 개선점에 대해 연구 활동을 진행하고 있다 [13].

2.3 AWS(Amazon Web Service) 구조

AWS는 아마존의 컴퓨팅 인프라에 프로그래밍 방식으로 액세스할 수 있도록 지원하는 서비스 집합이다 [2]. AWS는 대부분의 시스템에 반드시 필요한 기능인 스토리지, 컴퓨팅, 메시징 및 데이터세트를 제공하는 기본 빌딩 블록 서비스를 가지고 있다. 각 서비스의 상호 작용

은 표준 기반 SOAP(Simple Object Access Protocol) 및 REST(REpresentational State Transfer) 인터페이스로 이루어진다. 또한 신뢰할 수 있는 제 3자와 이들 서비스와의 통신을 위해 Ruby, Python, Java, Erlang, PHP 등을 포함한 여러 가지 언어로 작성한 개발자 라이브러리를 사용할 수 있다. 그림 1은 AWS의 시스템 구조를 나타낸다.

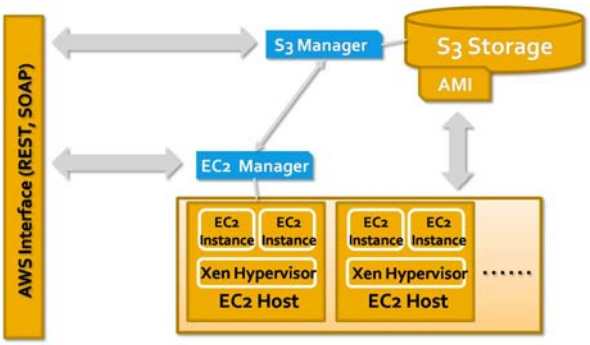

그림 1 AWS 구조

2.4 S3(Simple Storage Service)

아마존 S3는 데이터 저장 및 검색 기능을 갖춘 웹 서비스 인터페이스를 제공한다 [3, 6]. 데이터 유형에는 제한이 없으며 인터넷을 통해 어디에서나 데이터를 저장하고 액세스할 수 있다. S3에 저장할 수 있는 오브젝트의 수에는 제한이 없으며 저장할 수 있는 오브젝트의 범위는 1바이트 ~ 5GB까지이다. 스토리지 자체는 미국이나 EU(European Union)에 있으며 버킷을 만들 때 오브젝트를 저장할 스토리지 위치를 선택할 수 있다. S3에 저장한 각 오브젝트에는 액세스 제한을 지정할 수 있으며, HTTP 쿼리를 사용하여 오브젝트에 액세스 할 수 있다. 그림 2는 S3의 시스템 구조를 나타낸다.

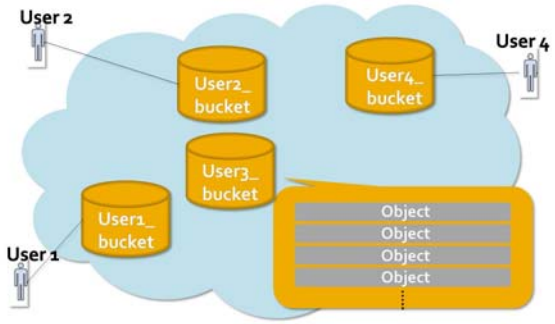

그림 2 S3 구조

III. 클라우드 스토리지 서비스에 대한 논의

본 장에서는 클라우드 컴퓨팅을 제공하는 벤더들에 대한 신뢰성에 관해 논의한다. 그리고 클라우드 컴퓨팅 스토리지 서비스인 S3에 대한 공격을 위한 기본 가정에 대해 살펴본다.

3.1 벤더 신뢰성

서비스를 제공하는 벤더를 신뢰할 수 있는지 아닌지는 클라우드 컴퓨팅 보안 연구에서 중요한 출발점이다. 개인에서 시작하여 소규모 벤처 또는 대기업에 이르기 까지 다양한 수요자들이 클라우드 컴퓨팅을 사용할 것이고 이들이 우려하는 가장 큰 문제는 과연 내 데이터가 안전하게 잘 보관되고 있는가에 대한 것일 것이다.

이에 관해 서비스 사용자들이 먼저 생각해야 할 것은 현재 자신이 클라우드에 저장하려는 데이터의 중요성이다. 클라우드 컴퓨팅 활용의 성공적인 사례로 자주 언급되는 New York 타임스의 신문 자료 디지털화 프로젝트에서 신문 자료란 모두가 열람할 수 있는 공용 자료이다. 하지만 회사 인사정보 같은 경우는 외부에서 열람 할 수 없어야 하고 유출 되었을 경우 파급효과가 큰 중요자료이다. 단순히 벤더에 대한 신뢰만을 가지고 클라우드 인프라에 쉽게 뛰어드는 것은 보안 측면에서 취약점을 발생시킬 수도 있다.

장차 클라우드 기술이 사회 전반에 없어서는 안 될 인프라가 될 것이라고 예상되고 있지만 그에 우선하여 클라우드 서비스 제공 벤더들에 대한 신뢰를 확립할 수 있는 방안에 대한 기술 및 정책 연구도 시급하다.

3.2 기본 가정

여기서는 4장에서 언급될 S3 서비스에 대한 공격을 위한 기본 가정에 대해 기술한다.

- 클라우드 스토리지 내에는 어떤 종류의 데이터도 저장 가능하다.
- DB내의 데이터는 암호화 되지 않은 평문 형태로 존재한다.

- 사용자는 HTTP 요청을 사용하여 버킷 및 오브젝트에 액세스가 가능하다.
- 사용자는 40바이트의 Secret Access Key와 20바이트의 Access Key ID를 부여받으며 이 두 개의 키를 사용하여 인증 프로세스를 거친다.

IV. 가능한 보안 위협

4장에서는 클라우드 컴퓨팅의 스토리지 서비스에 대해 가능한 보안 위협에 대해 살펴본다.

4.1 기밀성

아마존 S3 설계 명세서에 따르면 S3내에 저장되는 데이터는 암호화 되어 저장되지 않는다[1, 4]. 아마존에서는 중요한 데이터에 대하여 사용자가 직접 암호화 하여 저장 할 것을 권하고 있다. 위와 같은 권고가 지켜지지 않은 상태로 사용자 데이터가 관리될 경우 데이터의 기밀성이 보장되지 못한다.

4.2 서비스 거부 (Denial of Service) 공격

S3 스토리지 내의 데이터는 HTTP 요청을 통해 액세스가 가능하다. 이러한 특성은 NIWP(Norton Internet Worm Protection)의 사용과 연계되어, 어떤 사용자가 NIWP에 의해 필터링 당할 소지가 있는 파일을 S3 계정에 업로드 할 경우 해당 계정 소유자의 S3 서비스를 중단시킬 수 있다. 이 점을 악용하여 다음과 같은 과정을 거쳐 서비스 거부 공격이 가능하다.

① 악의적인 공격자는 S3를 저장소로 사용하고 있는 웹 사이트에 NIWP에 의해 필터링 될 소지가 있는 파일(예, ICC Profile Tagdata overflow)을 업로드 한다.
② 공격자는 위에서 업로드 한 파일을 다운받게 만드는 웹 페이지를 생성하고, 다른 사용자로 하여금 그 페이지를 방문하게 만든다.
③ 위에서 만든 웹 페이지가 열리면서 파일이 다운로드 될 것이고 사용자의 컴퓨터에 설치된 NIWP는 이러한 액세스를 시스템에 대한 공격으로 취급할 것이고 해당 IP를 블록할 것이다. 블록된 IP는 아마존 EC2내의 머신 인스턴스의 IP 주소이기 때문에 차후에 S3와 어떤 사용자간의 통신도 이루어지지 못한다.

4.3 중간자 공격(Man-in-the-Middle attack)

AWS의 Signature version 1은 HTTP 쿼리를 다음과 같이 서명한다.

① 쿼리를 '&'와 '=' character로 나누어 key-value pair값으로 나눈다.
② key값에 따라 pair를 소트한다.
③ key와 value를 함께 append하여 key1 + value1 + key2 + value2 +...과 같은 하나의 큰 스트링을 만든다.
④ 위의 스트링과 secret access key를 HMAC-SHA1으로 서명한다.

AWS Signature version 1은 다른 두 개의 메시지로부터 동일한 서명값을 생성하는 것은 계산적으로 불가능해야 한다는 암호학적 원칙을 간과하고 있다. AWS 서명 스킴을 보면 key와 value사이에 구획문자(delimiter)가 없기 때문에 "foo=bar"에 대한 서명은 "foob=ar"에 대한 서명과 동일하게 취급된다. 마찬가지로 "foo=bar&fooble=baz"를 위한 서명도 "foo=barfooblebaz"의 서명과 동일한 서명으로 확인된다.

공격자는 이를 악용하여 두 개의 다른 쿼리로부터 동일한 서명을 생성하여 악의적인 쿼리에 접합(attach)하여 정당한 쿼리인 것처럼 인증 받을 수 있다.

4.4 언급된 공격의 수행 가능성

4.2에서 언급된 서비스 거부 공격은 S3의 자체 결함이기보다는 웜 디텍션 툴과의 연계작용으로 인해 발생될 수 있는 공격이다. 근본적으로는 S3가 HTTP 쿼리를 통한 데이터 액세스를 허용하기 때문에 발생하는 것이지만 안티

웜 디렉션 툴 없이는 발생하기 어려운 공격이다. 그러나 이와 같은 공격의 성공률이 상당히 높으며 이 같은 취약점이 NIWP이외의 다른 안티 웜 디렉션 툴의 사용을 통해서도 발생할 수 있다는 점에서 볼 때, 추후 양쪽 S/W 개발 벤더에서 반드시 고려하여야 하는 사항이다.

4,3에서 언급된 공격은 일반적인 사용자보다는 악의적인 공격자에 의해 실행될 가능성이 높은 공격이다. 외부 공격자는 동일한 값을 가지는 복수의 서명을 생성하여 악의적인 쿼리에 접합하여 S3 데이터베이스를 공격할 수 있다.

V. 결론

본 논문에서는 아마존 웹 서비스 AWS의 스토리지 보안 위협에 대해 알아보았다. 아마존 웹 서비스의 스토리지 서비스를 담당하고 있는 S3는 대용량의 저장 공간을 제공하고 HTTP 쿼리를 통해 데이터에 대한 편리한 액세스 인터페이스를 제공한다.

하지만 데이터 액세스 쿼리에서의 서명 생성 과정에서 발생하는 충돌 가능성과 HTTP 쿼리 허용으로 인한 서비스 거부 공격의 가능성을 내포하고 있어 악의적인 공격자로부터의 보안 위협 가능성을 가지고 있다.

이에 본 논문에서는 위에서 언급한 취약점에 대해 분석하고 이를 이용한 두 가지 공격에 대해 제시하였다. 첫째, HTTP 쿼리를 통한 데이터 액세스를 허용함으로 인해 이를 악용한 서비스 거부 공격에 취약할 수 있다. 둘째, 각기 다른 두 개의 쿼리로부터의 서명값 생성에 충돌이 발생할 수 있어 이를 악용한 중간자 공격이 가능하다.

위에서 언급된 공격들은 악의적인 공격자뿐만 아니라 일반적인 사용자도 쉽게 수행할 수 있는 공격이기 때문에 그 심각성이 크다고 할 수 있다. 그러므로 클라우드 컴퓨팅에서의 안전한 저장장치 서비스를 위해 본 논문에서 언급된 취약점은 추후에 반드시 개선되어야 할 것이다.

[참고문헌]

[1] Amazon Web Services LLC, "Amazon Web Services: Overview of Security Processes", *Amazon White paper*, September, 2008.

[2] Jinesh Varia, "Cloud Architectures, Amazon Web Services", *Amazon White paper*, 2008.

[3] Simson Garfinkel, Commodity grid computing with Amazon's S3 and EC2, *USENIX,* February, 2007.

[4] Mayur Palankar, Ayodele Onibokun, Adriana Iamnitchi, and Matei Ripeanu, Amazon S3 for Science Grids: a Viable Solution?, *4th USENIX Symposium on Networked Systems Design & Implementation (NSDI'07)*, 2008.

[5] Simson Garfinkel, An Evaluation of Amazon's Grid Computing Services: EC2, S3, SQS, *Harvard University Technical report*, July, 2008.

[6] Michael Vrable, Stefan Savage, and Geoffrey M. Voelker, Cumulus: Filesystem Backup to the Cloud, *7th USENIX Conference on File and Storage Technologies (FAST '09)*, July, 2008.

[7] Michael Armbrust *et al*, "Above the Clouds: A Berkeley View of Cloud Computing", *UC Berkeley Technical report*, Feb, 2009.

[8] Won Kim, "Cloud Computing: Today and Tomorrow", *Journal OF Object Technology*, Feb, 2009.

[9] Greg Boss, Padman Malladi, Dennis Quan, Linda Legregni, and Harold Hall, "Cloud Computing", October, 2007.

[10] http://aws.amazon.com/ 아마존 AWS 웹 페이지

[11] http://www.azure.com/ 마이크로소프트 애저 플랫폼 웹페이지

[12] http://code.google.com/intl/ki/appengine/docs/ 구글 AppEngine 웹페이지

[13] http://www.kiisc.or.kr/ 한국정보보호학회 웹 페이지