클라우드 컴퓨팅에서 그레이웨어 역기능 최소화 방안 연구

김진덕, 김아란, 이재설
동양미래대학 네트워크정보통신학과
e-mail : gunduckv@may.dongyang.ac.kr
minimi1205, jslee@dongyang.ac.kr

A Study to way for minimize dysfunctional Grayware in Cloud-Computing

Jin-Duck Kim, A-Ran Kim, Jae-Sul Lee
Dept. of Network Information Communication, Dong-Yang Mirae University

요 약

Grayware 는 정상적인 소프트웨어와 달리 사용자의 동의가 없거나, 사용자가 인지하지 못하는상태에 설치되어 개인이나 기업의 특정정보를 수집하여 외부에 유출시키는 소프트웨어이다[1]. 최근에는 Grayware 가 지능적인 수법의 Crimeware 로 변질되어 감에 따라, 순기능보다 역기능이 증가하고 있으며, 그 중 개인정보 및 기업의 중요 데이터 유출의 심각성이 증가하고 있다. 본 논문에서는 클라우드 컴퓨팅을 이용하여 Multi-Factor 인증과 Anti-Grayware System(이하 Anti-G/W System)을 이용한 Grayware 역기능 최소화 방안을 제안한다.

1. 서론

IT 기술의 발전과 초고속 인터넷 보급이 증가 함에 따라 클라우드 컴퓨팅 환경의 발전이 이루어졌다. 그러나 이러한 발전과는 반대로 바이러스나 악성코드로 인한 개인 및 기업의 정보유출이 이전보다 심각한 상황에 마주하고 있다. 최근에는 Grayware 가 지능적인 수법의 Crimeware 로 변질되어감에 따라, 순기능보다 역기능이 증가하고 있으며 그 중 개인정보 및 기업의 중요 데이터 유출의 심각성이 증가하고 있다. 그리하여 본 논문에서는 클라우드 컴퓨팅의 가상화를 이용한 Grayware 의 역기능 최소화 방안을 제시하였다. 2 장에서는 Grayware 와 클라우드 컴퓨팅의 정의와 특징, 데스크탑 가상화에 대해서 서술하였고 3 장에서는 클라우드 컴퓨팅의 가상화를 이용한 Grayware 예방 및 대응 방안을 제안한다. 4 장에서는 기존 악성코드 대응기술과 본 논문에서 제안하는 Grayware 대응기술간의 성능평가가 이루어지며, 5 장에서는 결론과 향후 보완점에 대해서 설명한다.

2. 관련 연구

2.1 그레이웨어(Grayware)

Grayware 는 정상적인 소프트웨어와 달리 사용자의 동의가 없거나, 사용자가 인지하지 못하는 상태에 설치되어 개인이나 기업의 특정정보를 수집하여 외부로 유출시키는 소프트웨어이다[1].

기능	설명	역기능	순기능	호칭
추적	사용자 행위 또는 사용자 정보 관찰(수집)	개인정보 노출 ID 도난 컴퓨터 속도 저하 보안침해 기회제공	부모/기업의 합법적 관찰	Snoopware Keylogger
광고, 배너 디스플레이	광고성 컨텐츠 화면표시	성가심과 생산성 저장 불쾌한 컨텐츠 디스플레이 컴퓨터 속도저하	광고성 정보 제공	Adware
원격제어	원격 제어 또는 액세스	컴퓨터 자원 도용 대량 메일 발송 DDOS 공격 가담 옳란 자료 서비스	자신의 데이터에 대한 원격 액세스 원격 기술지원 및 고장수리	Backdoor Botnet Zombie Droneware
다이얼링	모뎀을사용한 원격 접속	전화료 부과	원격 서비스 액세스	Dialer
시스템 수정	시스템 또는 사용자 설정 변경	동의없이 시스템 무결성 훼손	시스템 커스터 마이징	Hijacker Rootkit
보안 분석	보안 상태 분석 및 우회	보안 침해	보안 연구 또는 합법적 보안 이행	Hacker Tool
자동 다운로딩	사용자 개입 없이 소프트웨어 다운로드/설치	비인가 소프트웨어 설치	자동 갱신 또는 시스템 자동 관리	Tricker

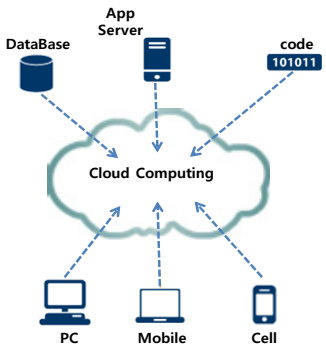
<표 1> Grayware 의 순기능과 역기능[3]

대표적인 기능은 추적, 광고배너 디스플레이, 원격제어, 다이얼링, 시스템 수정, 보안분석, 자동 다운로딩이 있다. 그러나 Grayware 는 이러한 순기능 이외에 개인정보를 유출하거나 ID 를 도난하며 보안 침해기회를 제공하고, 요청하지 않은 컨텐츠를 디스플레이 할 뿐만 아니라, 컴퓨터 속도저하를 가져오고 컴퓨터 자원도용 및 대량 메일발송, DDOS 공격 가담, 적절한

동의 없이 시스템 무결성훼손, 비인가 소프트웨어 설치 등의 역기능을 발생시키며 이로 인해 개인 및 기업에 막대한 피해를 입히고 있다. <표 1>은 Grayware의 순기능과 역기능을 나타낸다[3].

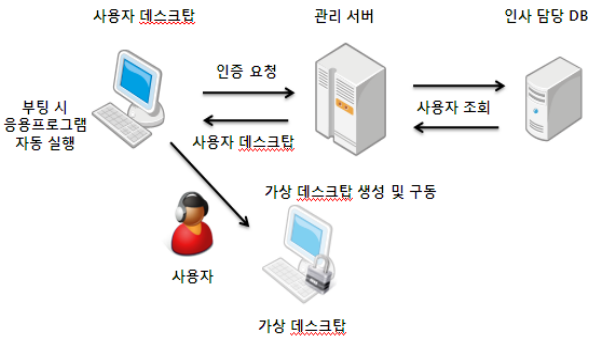
2.2 클라우드 컴퓨팅

클라우드 컴퓨팅은 인터넷을 기반으로 사용자들에게 높은 수준의 확장성을 가진 탄력 있는 IT 관련 기능 서비스를 제공하는 컴퓨팅의 방식이다[2].
(그림 1 과)같이 인터넷에 연결된 Device 를 통해 클라우드 컴퓨팅에 접속해 사용자가 원하는 서비스를 받을 수 있다. 최근에는 서버 가상화를 넘어서 서버와 데스크탑을 결합한 가상화 기술이 사용되고 있으며,여러 기업에서 다양한 기술을 선보이고 있다.



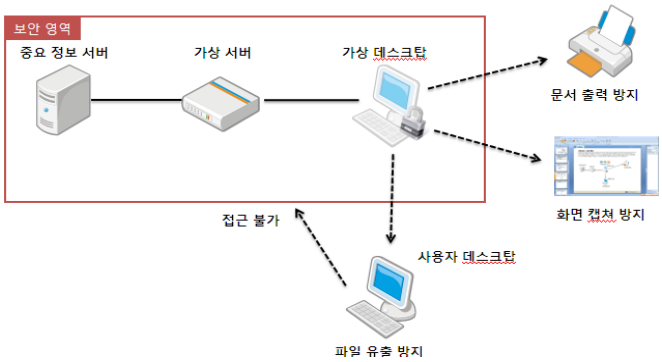
(그림 1) 클라우드 컴퓨팅 개요[7]

2.3 데스크탑 가상화



(그림 2)데스크탑 가상화의 개요[6]

데스크탑 가상화는 가상화된 데스크탑 화면을 사용자의 데스크탑 화면에 전송 받아 업무를 처리할 수 있는 환경을 제공한다.(그림 2)와 같이 사용자 데스크탑을 부팅 시 클라우드 환경에 접속하기 위해 필요한 특정 소프트웨어가 자동실행 되며 사용자들은 로그인 절차를 통해 관리서버에게 사용자의 인증요청을 하게 되며 관리서버는 인사담당 DB 로 사용자 조회 후 인증에 성공하면 사용자가 원하는 환경의 가상 데스크탑이 생성된다. 안전한 업무 처리를 위해 업무를 위한 응용프로그램들은 가상 데스크탑 내부에서 작동하며, 개인 및 기업의 중요 데이터는 가상서버를 거쳐, 암호화 과정을 지나 중요정보서버에 저장된다.
(그림 3)과 같이 중요데이터에 대한 접근은 가상 데스크탑 환경 안에서만 가능하고, 외부환경이나 다른 매체로 유출할 수 없으며, 문서 출력 및 화면 캡쳐 기능제한으로 철저한 보안 관리 및 데이터의 무결성을 보장할 수 있다

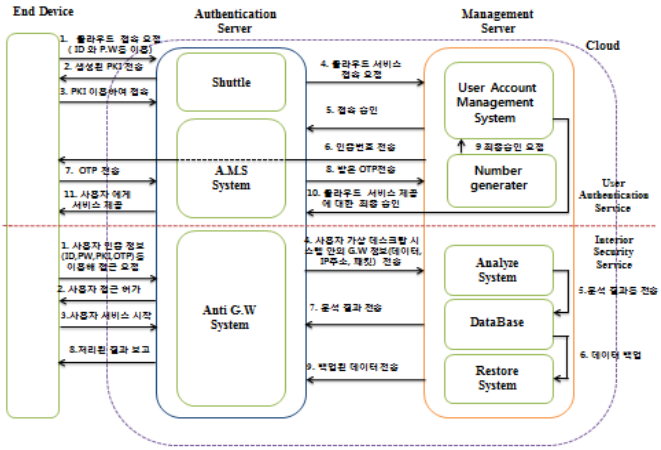


(그림 3)데스크탑 가상화 보안[6]

3. 제안하는 역기능 최소화 방안

3.1 역기능 최소화 방안 개요

Authentication Server(A/S) 와 Management Server(M/S)로 구성된 역기능 최소화 방안은 (그림 4)와 같다.



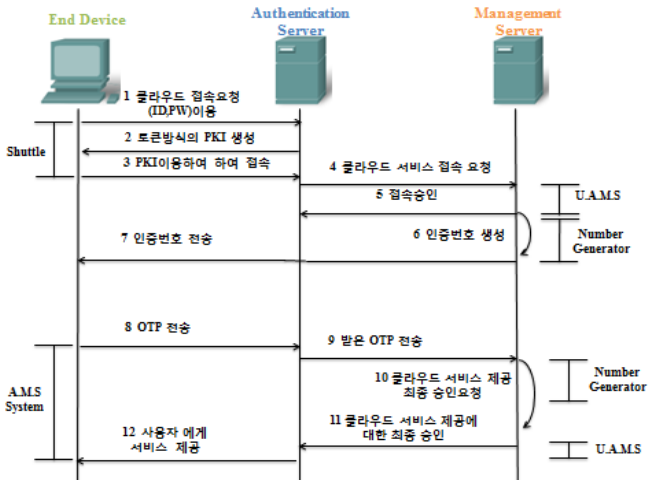
(그림 4)제안하는 역기능 최소화 방안의 개요

A/S 는 사용자 인증과 관련하여 접속요청에 대한 PKI 생성, OTP 전송 및 사용자에게 클라우드 서비스를 제공하며, 내부보안과 관련하여 역기능을 유발하는 Grayware 의 삭제 및 필터링 역할, 사용자에게 처리된 결과보고 등의 역할을 한다. M/S 는 사용자 인증과 관련하여, 사용자에게 인증번호 전송, 사용자 접속승인 관리를 담당하며, 내부보안과 관련하여 유해 Grayware

분석, 분석 데이터 저장 및 백업, 분석결과를 Anti-G/W System 에 전송하는 역할을 한다. 사용자가 A/S 에 클라우드 접속을 요청하면, A/S 는 사용자에게 PKI 를 전송하고 사용자는 PKI 를 이용해 A/S 에 접속하여 M/S 에 클라우드 서비스 접속요청을 하게 된다. M/S 는 접속승인 전송 후 사용자에게 인증번호를 전송하고, 사용자는 OTP 를 생성, A/S 를 거쳐 M/S 로 보낸다. M/S 가 클라우드 서비스 접속 최종승인을 A/S 로 보내며, A/S 에서 사용자에게 클라우스 서비스 제공을 시작한다. 사용자는 사용자인증정보를 통해 Anti G/W System 에 접속하며, Anti G/W System 은 사용자 가상 데스크탑 안의 Grayware 정보를 Analyze System 에 전송하고, 분석을 통해 분석결과를 Database 에 전송한다. Database 는 Restore System 에 분석결과를 백업하고, Anti G/W System 에 분석결과를 전송한다. Anti G/W System 은 전송 받은 정보를 바탕으로 유해 Grayware 의 처리결과를 사용자에게 실시간으로 전송한다. Restore System 은 백업된 데이터를 저장하고, 시스템 오작동 시 신속한 시스템 복구를 통해 피해를 최소화 시킨다.

. 3.2 사용자 인증 서비스

사용자 인증 서비스는 Shuttle, Number Gernerator(N/G), User Account Management(U/A/M/S),Approval Management Send System(A/M/S/S)로 (그림 5)와 같이 구성된다.

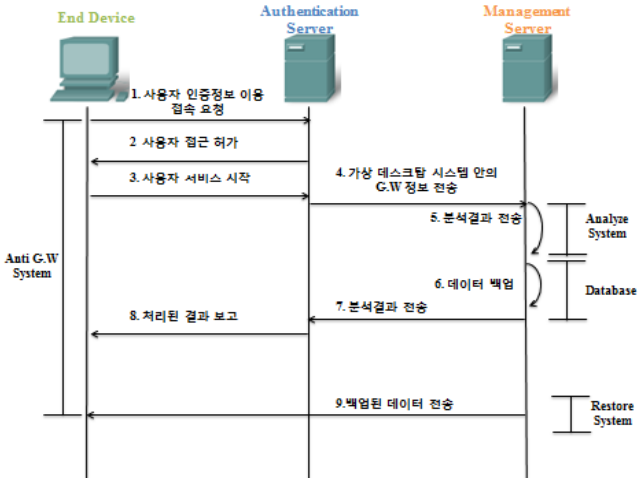


(그림 5) 사용자 인증절차

Shuttle 은 클라우드 접속 요청에 대한 PKI 생성 및 M/S 로 서비스 접속을 요청한다. A/M/S/S 는 사용자의 OTP 를 M/S 에 전송하고, 서비스 제공에 대한 최종 승인을 받아 사용자에게 서비스를 제공한다. U/A/M/S 는 사용자 계정을 관리하며, 최종승인 여부를 결정한다. N/G 는 사용자에게 인증번호를 전송하고 사용자의 OTP 를 확인해 U/A/M/S 에 최종 승인을 요청한다. 사용자는 ID 와 PW 를 이용해 클라우드 접속을 요청, Shuttle 은 사용자에게 PKCS#11 표준인 토큰방식 PKI(Public Key Infrastucture)를 생성, 사용자에 전송하고, 사용자는 PKI 를 이용하여 접속한다. Shuttle 은 U/A/M/S 에 클라우드 서비스 접속을 요청하고, U/A/M/S 에서 사용자 접속승인을 A/M/S/S 에 전송하며, N/G 는 사용자에게 인증번호를 전송한다. 사용자는 일회용 비밀번호인 OTP 를 A/M/S/S 에 전송하고, 다시 N/G 에 전송한다. N/G 는 클라우드 서비스 최종승인 요청을 U/A/M/S 에 보낸다. U/A/M/S 는 최종승인을 A/M/S/S 에 전송하며, A/M/S/S 에서 사용자에게 서비스를 제공한다. 이러한 Multi-factor 인증을 통해 사용자와 기업은 신뢰성 있는 접근이 가능하며, Keylogger 및 서버와 클라이언트 사이에서 중간자 공격을하는 MITM 공격에 보다 효과적인 대처가 가능하다.

3.3 내부 보안 서비스

내부 보안 서비스는 Anti G/W System, Database, Analyze System, Restore System 으로 구성되며, (그림 6)과 같다.



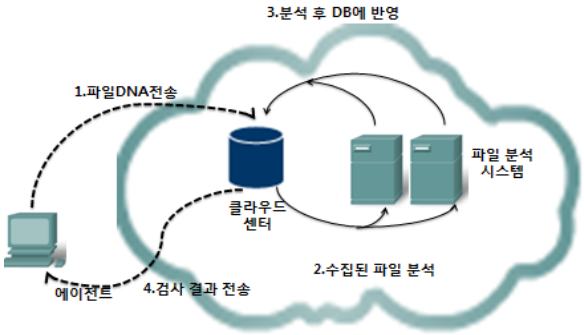
(그림 6)클라우드 컴퓨팅 내부 보안 시스템

Anti G/W System 은 사용자 가상 데스크탑 안의 유해한 Grayware 를 삭제하거나 Filtering 하고, 역기능이 의심되는 Grayware 정보를 Analyze System 에 전송하며, 사용자에게 결과를 보고한다. Analyze System 는 전송받은 Grayware 정보를 분석하여 Database 로 전송한다. Database 는 분석결과를 Anti G/W System 에 전송하고, Restore System 에 백업한다. Restore System 은 재해복구 시스템으로, Anti G/W System 이 비정상적으로 동작할 경우, 백업된 데이터를 보내 신속히 대응한다. 사용자는 클라우드 인증정보(ID, PW, PKI, OTP)를 이용해 Anti G/W System 에 접근을 요청한다. Anti G/W System 에서 사용자의 접근이 허가되면, 사용자는 서비스를 시작하고, Anti G/W System 은 자동 감염 시그니처 생성기술인 AGIS 를 적용하여, 사용자 가상 데스크탑 안의 의심되는 G/W 정보(데이터, IP 주소, 패킷) 를 Analyze System 으로 전송, 분석을 요청한다[4]. 분석을 마친 후 분석결과를 Database 로 전송한다. Database 는 받은 분석결과를 Restore System 으로 백업하고, Analyze System 으로 분석결과를 전송한다. 분석결과를

바탕으로 역기능을 초래하는 Grayware 일 경우, 자동 삭제 및 사전 Filtering 을 수행하여 역기능을 최소화 시킨다. Anti G/W System 으로부터 처리된 결과를 사용자는 실시간으로 보고받기 때문에 시스템에 대한 신뢰성을 확보할 수 있다. 또한 Anti G/W System 의 비정상적인 작동에 신속히 대응할 수 있도록, Restore System 에서 Anti G/W System 으로 백업데이터를 전송하여, 시스템의 신속한 복구를 수행한다.

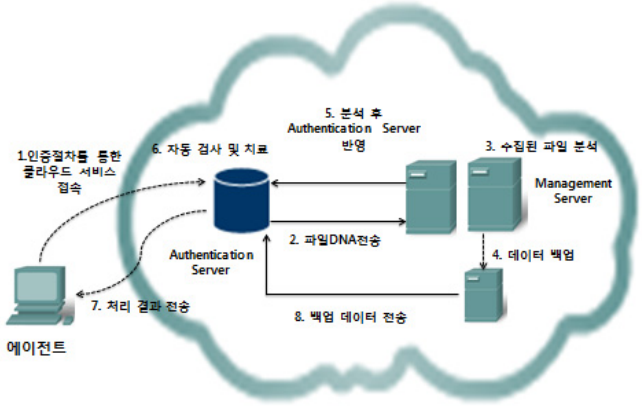
4. 성능평가

클라우드 기술도입을 통한 보안서비스 기술은 (그림 7)과 같이 에이전트에서 파일 DNA 를 클라우드 센터로 전송한다. 클라우드 센터는 파일분석 시스템으로 수집된 파일을 분석한다. 파일 분석시스템에서 분석된 정보는 DB 에 반영되며 클라우드 센터에서 에이전트로 검사결과를 전송한다[5].



(그림 7) 최근의 악성코드 대응기술[5]

반면 (그림 8)과 같이 제안한 데스크탑 가상화를 이용한 Grayware 대응 기술은 취약한 사용자의 데스크탑을 대신하여 데스크탑 가상화를 구현하였다.



(그림 8)데스크탑 가상화를 이용한 그레이웨어 대응 기술

<표 2> 는 Anti-G.W System 과 기존 보안시스템 비교분석을 나타낸다.

	사용자 인증	외부침입차단	재해 복구 (중요데이터백업)	가상화
Anti-G.W System	ID, PW, PKI	PKI	Restore System	데스크탑 가상화
기존 보안시스템	license	X	X	Web 기반, Software

<표 2> 제안 하는 시스템과 이전 시스템의 성능 평가

Multi-Factor(ID, PW, PKI)를 이용한 사용자인증을 통해 외부로부터 침입차단이 가능하고, Restore System 을 이용, 재해복구서비스를 제공하여 중요 데이터의 손상으로부터 신속히 복구가능하며, 데스크탑 가상화를 통해 사용자 데스크탑의 리소스 점유율을 감소시킨다. 기존 보안시스템과 비교해 볼 때 사용자 데스크탑의 가용성이 증가하였다.

5. 결론

본 논문에서는 클라우드 컴퓨팅에서 Grayware 역기능 최소화 방안을 제안하였다. Grayware 가 DDOS 공격가담, 개인정보 유출, 적절한 동의 없이 시스템 무결성 훼손 등의 역기능을 동반하고 있는 만큼 적절한 대응조치가 필요하며, 이에 대응하기 위한 데스크탑 가상화를 통해 사용자가 시스템 접근시 Multi-factor 인증 방식으로 중요데이터 및 시스템에 대한 사전 침입차단이 가능하고, 보다 신뢰성 있는 접근이 가능하다. 그러나 클라우드 컴퓨팅의 오류 발생시 시스템의 오작동 등의 문제점들이 그대로 노출되기 때문에 클라우드 컴퓨팅의 취약점 분석을 통한 대응방안 및 보호 대책에 대한 선행 연구와 함께 전화료 부과, 음란자료 서비스 등의 Grayware 의 다른 역기능에 대한 대응방안이 모색되어야 할 것이다.

참고문헌

[1]http://en.wikipedia.org/wiki/Grayware#Grayware
[2]http://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_CloudComputing.pdf.
[3] KISA-한국정보보호진흥연구원. “유해 그레이웨어(Grayware)위협에 대한 분석 및 대응 2006 년 8 월.
[4] Crimeware: Understanding New Attacks and Defenses /Markus Jakobsson , Zlfikar Ramzan , Feb. 2008.
[5]권진욱. “클라우드 기술도입을 통한 보안서비스의 새로운 패러다임”. TTA Journal, 2009 년 10 월.
[6]신상윤. “클라이언트 가상화 기반 중요정보 유출방지 솔루션 제안”. 2009 년 5 월.
[7]http://rdmcommunity.blogspot.com/2010/07/working-in-clouds.html
[8] 김현승, 박춘식. “클라우드 컴퓨팅과 개인인증 서비스”. 정보보호학회지 제 20 권 제 2 호. 2010 년 4 월