윈도우즈 시스템의 보안 강화를 위한 정책 제어 시스템 설계

박정진° 박진섭 이승혁 백승덕
대전대학교 (주)유비엔씨
parkjj°@ubnc.net, jspark@dju.ac.kr {leesh, bsd}@ubnc.net

Design of Policy control system for Security enhancement of the Windows Systems

Jungjin Park°, Jinsub Park, Seunghyeok Lee, Seungduk Baek
Daejon University, UBNC Corp

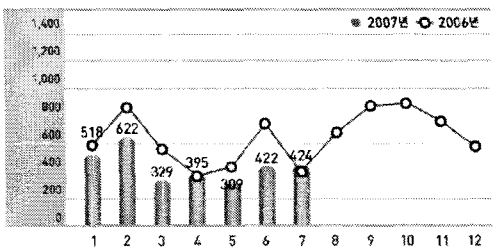
요 약

인터넷 및 네트워크의 사용이 일반화됨으로써 컴퓨터 시스템을 사용하지 않는 분야 및 사용자가 없을 정도이다. 컴퓨터 시스템을 사용함에 있어 순기능이 있는 반면 이에 대한 역기능 또한 급속하게 증가하고 있다. 역기능 중 가장 심각한 문제를 발생시킬 수 있는 부분이 웜 및 바이러스, 또한 악의적인 목적이 해킹 등이 있다. 이러한 문제를 해결하기 위해 각종 보안시스템 및 소프트웨어를 도입하여 사용하고 있지만 이에 앞서 일반적으로 사용하는 윈도우즈 시스템 자체에 포함되어 있는 각종 보안 설정을 통하여 근본적인 원인을 해결할 수 있다면 악의적인 목적에 의한 피해는 미연에 방지할 수 있을 것이다. 본 논문에서는 이러한 윈도우즈 시스템 자체에 있는 보안설정 기능을 자동으로 설정 및 제어할 수 있는 시스템을 제안하고자 한다.

1. 서 론

컴퓨터 시스템의 보급과 인터넷의 대중화는 현재의 생활에 엄청난 변화를 가져왔다. 일상생활에서 인터넷 및 컴퓨터가 없다는 것은 상상도 할 수 없을 정도로 그에 대한 의존도가 높아지고 반드시 없어서는 안 될 환경이 되었다.

컴퓨터 시스템을 사용하면서 많은 유용한 기능을 통하여 업무의 효율성을 극대화하고 편리함을 누릴 수 있게 되었다. 그러나 컴퓨터를 사용함에 있어 우리는 다양한 위협에 노출되어 있다. 최근 가장 많은 위협으로 여겨지는 웜 및 바이러스가 그 예이다. 또한 악의적인 목적으로 타인의 시스템에 불법적으로 침입하여 이득을 노리는 해킹 또한 빈번하게 발생하고 있다. [그림 1]에서 국내의 웜 및 바이러스의 발생 동향을 보이고 있다.



[그림 1] 월별 국내 웜 및 바이러스 신고건수
출처: 한국정보보호진흥원 인터넷침해사고대응지원센터

이러한 웜 및 바이러스, 해킹 등은 일반인들이 쉽게 해결할 수 있는 일이 아니다. 이러한 문제를 해결하기 위해 대부분의 조직 및 개인은 안티바이러스 소프트웨어 및 각종 네트워크 보안 장비 등을 도입하여 운영하고 있다.

그러나 이러한 보안 장비 및 소프트웨어를 도입하여 운영하는 것은 문제가 발생했을 경우 해결하기 위한 방법이거나 내부 네트워크에서 발생하는 문제를 해결하는 데는 그 한계가 있다. 웜 및 바이러스, 해킹은 윈도우즈 시스템의 보안 취약성을 이용하기 때문에 이러한 보안 취약성을 제거한다면 악의적인 프로그램 및 해킹으로부터 근본적인 원인을 제거하는 것이다[1].

따라서, 본 논문에서는 웜 및 바이러스, 해킹 등의 근본적인 원인인 윈도우즈 시스템의 보안 취약점을 해결하기 위해 윈도우즈 시스템 자체가 가지고 있는 다양한 보안 설정 기능을 제어할 수 있는 시스템을 설계하고자 한다.

1장의 서론에 이어, 2장에서는 제안하는 시스템과 관련된 기술 등에 대한 내용을 서술하고 3장에서는 본 논문에서 제안하고자 하는 시스템에 대한 내용을 서술한다. 그리고 마지막 4장에서는 본 논문의 결론을 기술한다.

2. 관련 기술 및 연구

2.1 보안 취약성 진단 기술

보안 취약점(Vulnerability)이란 정보시스템에 불법적인 사용자의 접근을 허용할 수 있는 위협, 정보시스템의 정상적인 서비스를 방해할 수 있는 위협, 정보시스템에서

관리하는 중요한 데이터의 유출 및 변조, 삭제 등에 대한 위협을 말한다[2].

취약성 분석 시스템은 네트워크나 시스템상의 보안 취약성을 진단하고 분석하여 그 결과를 바탕으로 해결방법을 제시해주는 시스템을 말한다. 이러한 보안 취약성 시스템은 일반적으로 취약점에 대한 정보와 개별방법을 제시하지만 취약점을 직접적으로 해결하지는 않는다.

국내외의 보안 취약성 진단 시스템으로는 국내의 나일소프트사의 SecuGuard SEE(System Security Explorer), 시큐아이닷컴의 SecuiSCAN과 국외로는 DISA Gold Disk와 Microsoft사의 Baseline Security Analyzer(MBSA) 등이 있다.

3. 제안 시스템

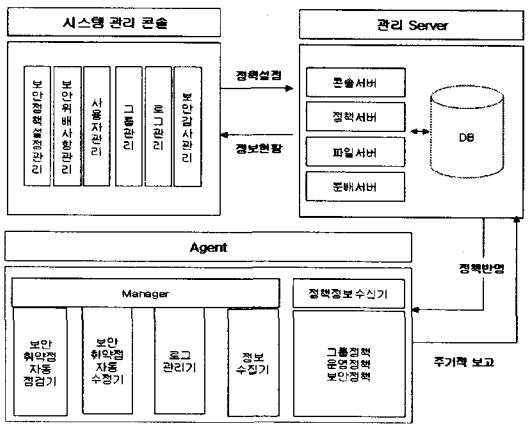
3.1 제안 시스템 개요

본 논문에서는 웜 및 바이러스, 해킹 등의 근본적인 원인이 되는 윈도우즈 시스템의 취약성 및 보안설정을 서버/클라이언트의 구조를 통하여 서버 측의 관리자가 에이전트가 설치된 윈도우즈 시스템(에이전트)을 강제적이고 자동적으로 제어할 수 있는 시스템을 제안한다.

일반적으로 윈도우즈 시스템 자체가 가지고 있는 다양한 보안 설정은 관리 기능을 통해 쉽게 설정할 수 있는 항목도 있지만, 많은 보안 설정들이 복잡하거나 쉽지 않은 방법을 통해서만 제어할 수 있도록 되어 있다[3][4].

제안하는 시스템에서는 윈도우즈의 계정 정책, 네트워크 관련 보안 정책, 시스템 관리 관련 보안 정책, 패치 관리 정책 등을 제어할 수 있도록 설계한다.

[그림 2]는 제안하는 시스템의 전체 구조를 나타낸다.



[그림 2] 시스템 구조

3.2 보안 정책 항목 정의

에이전트의 윈도우 시스템에서 점검될 항목은 일반적으로 시스템 사용자가 정책의 설정 유무를 판단하기 어렵고, 취약한 설정에 대해서 안전하도록 설정하기 어려운 항목을 중심으로 정의한다. 정의한 점검 항목들은 각각의 특성에 따라서 윈도우 계정 관리 기능, 공유폴더 관리 기능, 레지스트리 제어 기능, 서비스 제어 기능을 통해서 점검하고 권고되는 값으로 설정한다.

에이전트의 점검 대상이 되는 보안정책 카테고리 및 세부 항목은 [표 1]과 같다.

[표 1] 설정 대상 항목

정책 Category	세부 항목
사용자계정 관련 보안정책	- 로그온 패스워드 점검 - 최대 패스워드 사용기간 정책 점검 - 최소 패스워드 길이 정책 점검 - 최근 패스워드 기억 정책 점검 - 패스워드 만료 설정 점검 - Guest계정 점검
네트워크 관련 보안정책	- 관리용 공유폴더 설정 점검 - 사용자 공유폴더 설정 점검 - 윈도우즈 방화벽 점검 - Alert서비스 점검 - Computer Browser 서비스 점검 - Fast User Switching Compatibility 서비스 점검 - Messenger 서비스 점검 - Netmeeting Remte Desktop Sharing 서비스 점검 - Telnet 서비스 점검
시스템관리 관련 보안정책	- 자동 로그온 점검 - 화면보호기 활성화 설정 점검 - 화면보호기 자동실행 시간 점검 - 화면보호기 화면 잠금 설정 점검 - 자동 업데이트 점검 - Outlook Express 미리보기 설정 점검 - Outlook Express 메일 전송 경고 설정 점검 - Outlook Express 제한된 영역 설정 점검

3.3 에이전트 설계

에이전트는 서버에서 관리자에 의해 정책적으로 설정된 보안 정책을 수행하고 보고하는 기능을 한다. 에이전트의 동작 흐름은 에이전트가 프로그램이 초기 설치되면서 에이전트임을 확인할 수 있는 각종 시스템 정보를 수집하여 서버에 전송하고, 서버로부터 보안정책을 수행할 정책파일을 전송받는다. 정책 파일은 사용자 계정관련 파일(Account.ini), 네트워크 관련 정책 파일(Network.ini) 그리고 시스템관리 관련 정책 파일(Maintenance.ini) 파일로 정의된다. 에이전트에서는 수신한 정책파일의 보안점검 프로파일을 기반으로 에이전트 시스템의 보안 상태를 점검한다. 보안 상태를 점검한 후 결과 파일과 로그파일을 생성하여 관리 서버로 전송한다[5][6].

```
[ITEM_002]
title=최대 패스워드 사용 기간 정책 점검
comment=로그온 패스워드를 장기간 동일한 패스워드를 사용하면 제3자에게
level=3              # 1 - critical, 2-danger, 3-warning, 4-notice
auto_check=true
insp_type=account
acc_check_type=pass_period# 비밀번호 기간
check_type=range
from=30                    # 최소 30일
to=90                      # 최대 90일
auto_correct=true
correct_type=set
warning=true
guide=2.htm
```

[그림 3] Account.ini 정책 프로파일 예제

```
[ITEM_003]
title=Windows 방화벽 점검
comment=Windows XP SP2부터는 Windows 방화벽이 기본적으로 제공됨
level=1              # 1 - critical, 2-danger, 3-warning, 4-notice
auto_check=true
insp_type=registry
dependancy=os
target_os=WinXP_SP2
reg_path=HKLM₩System₩CurrentControlSet₩Services₩SharedAccess'
reg_key=EnableFirewall
reg_data_type=integer
check_type=limit    # value가 1 이어야 정상
from=1
auto_correct=true
correct_type=set
default_value=1
guide=9.htm
```

[그림 4] Network.ini 정책 프로파일 예제

```
[ITEM_002]
title=화면보호기 활성화 설정 점검
comment=사용자가 일정시간 컴퓨터를 사용하지 않을 경우 모니터
level=2              # 1 - critical, 2-danger, 3-warning, 4-notice
auto_check=true
insp_type=registry
reg_path=HKCU₩Control Panel₩Desktop
reg_key=ScreenSaveActive
reg_data_type=string_integer
check_type=limit    # value가 1 이어야 정상
from=1
auto_correct=true
correct_type=set
default_value=1
guide=12.htm
```

[그림 5] Maintenace.ini 정책 프로파일 예제

각각의 카테고리별 프로파일의 내용은 [그림 3], [그림 4], [그림 5]와 같다. 프로파일에서는 해당 점검 항목에 대한 상세 정보와 위험 수준, 해당 항목에 대해 자동으로 점검을 수행할 지에 대한 여부, 해당 항목에 대한 조치를 자동으로 수행할지에 대한 여부, 설정 값, 해당 항목에 대해 지정된 값으로 설정할지 해당 정보를 제거할지 여부 등에 대한 정보를 포함하고 있다.

에이전트는 정책 프로파일을 기반으로 시스템의 보안 상태를 점검하고 점검 결과를 서버로 전송한다. 에이전트가 생성하는 점검 결과 정보는 각각의 점검 항목에 대해 수행한 결과를 다양한 형태로 정의하여 해당 항목에 대한 정확한 정보를 생성한다[7].

[표 2] 점검 결과 상태 정의

Result Define	Comment
IR_NOT_CHECKED	점검수행 전
IR_CHECKED	점검완료 (안전)
IR_FAILED	점검실패
IR_DANGER	점검완료 (위험)
IR_MODIFIED	점검완료 및 수정됨
IR_MOD_FAILED	점검완료 및 수정실패
IR_RECOVERED	복구완료
IR_RECOVER_FAILED	복구오류
IR_NOT_SUPPORT	현재 시스템은 지원하지 않음

[표 2]에서는 에이전트가 보안 정책을 점검한 후 각각의 점검 항목에 대해 저장하는 형식을 정의한 것이다. 이를 통해 서버의 관리자는 에이전트에서 수행한 점검 결과를 통해 에이전트의 보안 설정 상태를 명확하게 파악할 수 있다. 또한 에이전트는 점검을 완료한 후 정책에 위배된 내용을 수정한 후 로그 데이터로 저장하여 서버로 그 내용을 전송한다[8][9]. [그림 6]은 에이전트에서 생성한 보안정책 수정 사항을 로그파일로 저장하고 있는 형태를 보이고 있다.

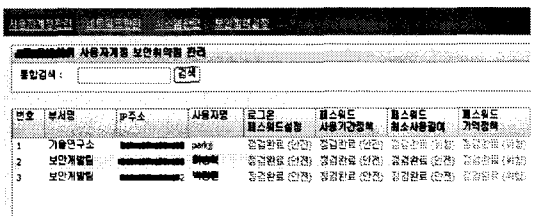
```
2007-08-21 21:33:12 '화면보호기 활성화 설정 점검'
        [HKEY_CURRENT_USER₩Control Panel₩Desktop]
        [ScreenSaveActive]의 값 '0'을 '1'으로 변경
2007-08-23 20:35:28 '화면보호기 활성화 설정 점검'
        [HKEY_CURRENT_USER₩Control Panel₩Desktop]
        [ScreenSaveActive]의 값 '0'을 '1'으로 변경
2007-08-23 20:35:28 '화면보호기 자동실행 시간 설정 점검'
        [HKEY_CURRENT_USER₩Control Panel₩Desktop]
        [ScreenSaveTimeOut]의 값 '600'을 '300'으로 변경
2007-08-23 20:35:28 'Outlook Express 미리보기 설정 점검'
        [HKEY_CURRENT_USER₩Identities₩{CB6BFDEC-4186-4928-
        [ShowHybridView]의 값 '1'을 '0'으로 변경
```

[그림 6] 에이전트 보안설정 변경 로그

3.4 서버 시스템 설계

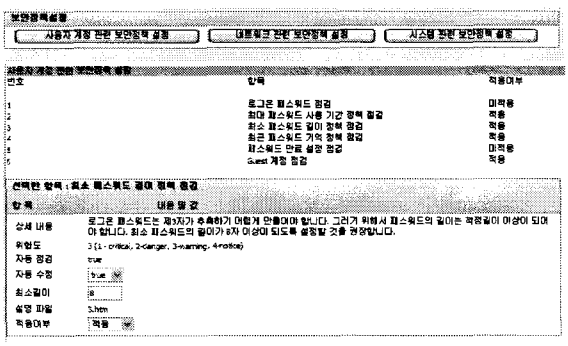
서버 시스템은 서버 데몬과 웹 관리 콘솔, 데이터베이스, 웹서버로 구성된다. 서버 데몬은 에이전트와의 통신 기능을 담당한다. 에이전트가 자신에 해당하는 정책을 요청하면 서버 데몬은 해당 에이전트에 부여된 정책 및 정보를 전송하고 에이전트에서 전송된 모든 정보를 데이터베이스에 저장하고 관리한다. 웹 관리 콘솔은 데이터베이스에 저장된 정보를 기반으로 관리자에게 정책 정보 및 에이전트 시스템 정보를 분석하고 확인할 수 있도록 인터페이스를 제공한다. 또한 관리자가 모든 정책을 생성, 수정, 삭제할 수 있는 인터페이스를 제공한다.

[그림 6]에서는 에이전트에서 수행된 보안 설정 점검에 대한 결과 중 사용자 계정 관련 점검 결과를 웹 관리 콘솔을 통하여 보이고 있다.



[그림 7] 사용자계정관련 정책 현황

웹 관리 콘솔에서는 에이전트에서 수행될 보안 점검 항목에 대한 세부적인 정책설정이 가능하도록 설계하였다. [그림7]에서 보는 바와 같이 해당 정책이 에이전트에서 자동으로 점검되고 위배항목에 대해 자동으로 수정을 할지 여부에 대한 설정과 각각의 항목마다 기본 값을 설정하도록 설계하였다. 또한 해당 정책 항목을 에이전트에 적용할지 적용하지 않을 지에 대한 판단도 보안 정책설정을 통하여 수행한다.



[그림 8] 보안정책 설정 인터페이스

4. 결 론

본 논문에서는 컴퓨터 시스템을 사용함에 있어 위협이 될 수 있는 웜 및 바이러스, 해킹 등의 행위에 대해 근본적인 원인을 윈도우즈 시스템 자체에서 설정 가능한 보안 설정기능을 통하여 1차적으로 예방할 수 있는 시스템을 제안하였다.

제안 시스템을 통하여 일반적으로 취급하기 어려운 윈도우내의 보안설정을 전문적인 관리자가 권고하고 설정하는 기준에 따라 시스템 사용자의 개입 없이 정책적으로 자동 설정되도록 하였다. 본 시스템을 적용함으로써 정보 시스템 사용자는 악의적인 외부 행위에 대하여 근본적인 원인을 제거함으로써 지속적이고 안정적으로 시스템의 안정성을 확보할 수 있다.

본 논문에서 제안 시스템과 함께 안티바이러스 프로그램 및 개인 방화벽 제품 등을 함께 사용한다면 악의적인 행위를 미연에 방지함과 동시에 발생한 위협에 대해서도 효과적으로 대응함으로써 시스템의 안정성을 최대한으로 유지할 수 있을 것이다. 또한 시스템 내에 저장된 중요 파일 데이터의 파괴 및 유출을 방지함으로써 중요 기술 및 경제적인 피해 또한 최소화 할 수 있을 것이다.

[참고문헌]

[1] http://www.secuve.co.kr

[2] Jungjin Park, Jinsub Park, Bonghoi Kim. "Windows Security Patch Auto-Management System Based on XML" The 9th ICACT. 2007

[3] 서명국, 송현교, 신영석. 보안정책 정보모델링과 보안정책 관리구조. 호남대학교 대학원 논문집. 2004

[4] 이동영, 김동수, 정태명. 이종의 보안시스템 관리를 위한 정책 기반의 통합보안관리시스템의 계층적 정책모델에 대한 연구. 정보처리학회. Vol.8-c No.5. 2001

[5] 손우용, 송정길. 통합보안 관리시스템의 침입탐지 및 대응을 위한 보안 정책 모델. 한국컴퓨터정보학회. Vol.9 No.2. 2004

[6] 박진섭. 네트워크 서비스 환경에서의 방화벽 보안정책. 대전대학교 산업기술연구소. Vol.8 No2. 1997

[7] 박진섭, 김봉희. 베이스라인 보안정책을 위한 위험분석 체크리스트. 대전대학교 산업기술연구소. Vol.8 No.2. 1997

[8] 김광혁, 권윤주, 김동수, 정태명. 통합보안관리 시스

템의 방화벽정책 분배를 위한 알고리즘. 정보처리학회. Vol.9-c No.4. 2002

[9] 한승오, 김영대. 정보시스템의 정보보호를 위한 보안체제에 관한 연구. 호남대학교 대학원. Vol.4. 2004