通信情報保護學會論文誌
第 7 卷 第 3 號, 1997. 9

지킴이: 유닉스 시스템을 위한 통합 보안 점검 도구

채 홍 석*, 이 남 희*, 김 형 호*, 김 내 희*, 차 성 덕*,
백 석 철**, 임 규 건**, 박 승 민**, 정 종 윤**

Zkimi: Integrated Security Analysis Tool for UNIX Systems

Heung Seok Chae, Nam Hee Lee, Hyung Ho Kim, Nae Hee Kim, Sung Deok Cha
Seok Chul Baek, Gyu Geon Lim, Seung Min Park, Jong Yoon Chung

요 약

지금까지 유닉스 시스템의 보안을 점검하거나 향상시키기 위하여 다양한 보안 도구들이 공개 소프트웨어(public domain)로 개발되어 사용되었다. 그러나, 대부분의 보안 도구들은 편리하고 일관성 있는 사용자 인터페이스를 제공하지 않으며, 또한 시스템의 특정 부분에 대 한 점검 기능만을 제공한다. 따라서, 시스템의 전반적인 보안을 관리해야 하는 시스템 관리자는 사용하기 불편한 여러 개의 도구들을 함께 사용해야 한다. 게다가, 이러한 도구들은 영어권에서 개발되었기 때문에, 국내의 현실이 잘 반영되지 않는 면이 있다.

본 논문에서는 사용하기 편리하면서 시스템의 전반적인 보안 점검 기능을 제공하는 통합 보안 점검 도구로서 "지킴이"를 구현하였다. 지킴이는 시스템의 전반적인 보안 점검을 위한 계정 보안, 시스템 보안, 네트웍 보안, 화일 변경 검사 기능과, 관리자의 정기적인 시스템 관리를 효율적으로 지원하기 위한 주기적인 보안 점검 기능을 제공한다. 지킴이의 각 기능은 기존의 공개된 대표적인 보안 도구를 바탕으로 하였으며, 기존 도구들의 단순한 조합이 아니라, 시스템 전체의 보안을 위해 필수적인 기능을 제공하도록 구성하였다. 그리고, WWW를 바탕으로 하는 사용자 인터페이스를 제공하기 때문에, 사용자는 기존의 WWW 브라우저를 이용하여 시스템의 전반적인 보안 상태를 점검할 수 있다. 또한, 지킴이를 실제 운용 중인 유닉스 시스템의 보안 상태를 점검하기 위하여 적용하였으며, 이를 통해서 지킴이의 효용성을 확인하였다.

Abstract

There are a lot of security tools for the investigation and improvement of UNIX systems. However,

* 한국과학기술원 전산학과
* * 한국통신 멀티미디어 연구소 네트웍 보안 연구팀

most of them fail to provide a consistent and usable user interface. In addition, they concentrate on a specific aspect of a system, not the whole one. For the overall management, system administrators cannot help using several uncomfortable tools. This paper introduces an integrated security analysis tool, named "Zkimi", which provides a convenient user interface and investigates the various aspects of UNIX systems such as account security, system security, network security, and file system integrity. The Zkimi supports user-friendly WWW based interface, so administrators can examine the various aspects of system more easily. We tried the tool for a system of a moderate size, and were confirmed that the tool is very efficient for investigating various security aspects of a system.

1. 개 요

전산망 사용의 급격한 증가와 더불어, 시스템의 결점을 이용한 자료의 불법 취득, 자료 파괴, 해킹 등이 심각한 문제로 제기되고 있다.[8] 컴퓨터의 사용과 전산망의 이용이 더욱 증가되는 현실임을 감안할 때, 이 문제는 앞으로 더욱 악화될 것이므로, 시스템의 보안은 불가피한 문제이다.

유닉스 시스템의 보안[3, 4, 6, 7, 10, 11]을 점검하거나 향상시키기 위하여 지금까지 다양한 보안 도구들이 개발되고 사용되어 왔다.[2, 5, 12] 그러나, 이러한 보안 도구들은 세가지 면에서 시스템 관리자가 실제로 시스템의 보안을 점검하기 위해 사용하기에 어려운 점이 있다. 첫째로, 기존의 보안 도구들은 편리한 사용자 인터페이스를 제공하지 않기 때문에, 일반적인 시스템 관리자가 사용법을 익히기가 쉽지 않으며, 이는 지속적인 시스템 관리에 장애 요소로 작용한다. 둘째로, 각 도구들은 시스템의 보안에 관련된 여러 가지 면 중에서 특정 부분만을 점검한다. 예를 들어, Tripwire는 시스템의 여러 가지 화일의 변경 사항에 대한 분석과 보고 기능만을 제공하며, SATAN과 ISS는 네트웍과 관련된 부분만을 점검한다. 따라서, 시스템의 전반적인 보안을 책임져야 하는 시스템 관리자는 사용하기 불편한 여러 가지 도구들을 익히고, 함께 사용할 수 밖에 없다. 마지막으로, 기존의 보안 도구들은 영어 문화권에서 개발되었기 때문에, 우리나라 환경에서 사용하기 불편하거나, 부족한 면을 가지고 있다. 예를 들어, 패스워드 크래킹의 경우 한글 단어를 패스워드로 많이 사용하는 우리나라의 현실을 기존의 패스워드 크래킹 도구들은 반영하지 못하고 있다. 따라서, 이러한 한국적인 환경을 잘 반영하고, 시스템의 여러 가지 면을 점검하며, 편리한 사용자 인터페이스를 제공하는 통합 보안 도구의 필요는 절실하다.

전체적인 시스템의 보안을 점검하기 위해 필수적인 점검 사항들을 바탕으로, 시스템의 여러 가지 면을 점검하고, 편리한 사용자 인터페이스를 제공하는 통합 보안 점검 도구 - "지킴이" - 를 설계 및 구현하였다. 또한, 실제 운용 중인 유닉스 시스템에 지킴이를 실제로 적용하여 그 효용성을 확인하였다.

지킴이는 시스템의 전반적인 보안 문제를 점검하기 위하여 보안 기능을 네 가지 범주 - 계정 보안, 시스템 보안, 네트웍 보안, 화일 변경 검사 - 로 나누었다. 또한, 시스템 관리자의 정기적인 시스템 점검을 편리하게 할 수 있도록 주기적인 보안 점검 기능도 제공한다.

지킴이는 각 기능별로 기존의 공개된 대표적인 보안 도구를 바탕으로 하여, 기존의 기능을 부분적으로 개선하거나 확장 시켰다. 또한, 사용자의 편의를 위하여 WWW를 바탕으로 하는 사용자 인터페이스를 제공한다. 따라서, 사용자는 지킴이를 이용하여 시스템에 대한 다양한 보안 점검을 수행할 수 있으며, 점검을 통해 얻

은 결과에 대한 자세한 온라인 설명을 통해서 시스템이 가진 문제점을 파악할 수 있다.

본 논문의 구성은 다음과 같다. 2절에서는 지킴이의 특징과 기능에 대하여 설명하고, 지킴이에 대한 설계와 실제 적용 사례를 3절과 4절에서 각각 기술한다. 5절에서는 지킴이의 개선점 또는 확장 가능성에 대하여 설명을 한다.

2. 지킴이 : 통합 보안 점검 도구

지킴이는 시스템 관리자들이 시스템의 보안에 관련된 전반적인 사항을 쉽고, 효과적으로 점검할 수 있도록 제안되었으며 다음과 같은 특징을 가진다.

- 전반적인 시스템에 대한 점검 기능 제공
  지킴이는 시스템의 전반적인 사항을 위하여 네 가지 범주 - 계정 보안, 시스템 보안, 네트웍 보안, 화일 변경 검사 - 로 나누어 점검을 수행한다. 그리고, 시스템 관리자에게 지속적인 보안 점검에 대한 편의성을 제공하기 위하여 주기적인 보안 점검 기능을 제공한다.

범 주	점 검	항목관련 도구
계정 보안	패스워드 화일 검사	COPS
	그룹 화일 검사	COPS
	패스워드 크래킹	Crack
시스템 보안	사용자 검사	COPS
	자동수행 화일 검사	COPS
	장치 화일 검사	COPS
네트웍 보안	인터넷 서비스 검사	COPS, SATAN
	Mail 서비스 검사	COPS, SATAN
	FTP 서비스 검사	COPS, SATAN
	TFTP 서비스 검사	COPS, SATAN
	NFS 서비스 검사	COPS, SATAN
	NIS 서비스 검사	COPS, SATAN
화일 변경 검사	화일의 생성, 변경, 삭제	Tripwire
주기적인 보안 점검	점검 항목의 정기적인 수행	

표 1 : 지킴이의 점검 항목

- 편리한 사용자 인터페이스와 온라인 설명 제공
  지킴이는 WWW를 바탕으로 사용자 인터페이스를 제공하므로, 사용자는 기존의 WWW 브라우저를 통하여 다양한 점검을 수행할 수 있다. 또한, 시스템에 대한 점검을 수행한 후, 발견된 문제에 대한 설명과 대책을 온라인으로 제공함으로써, 사용자는 쉽고 명확하게 문제를 파악하고 대처할 수 있다.

지킴이는 각 기능별로 기존의 대표적인 보안 도구를 바탕으로 하였으며, 기존 도구들의

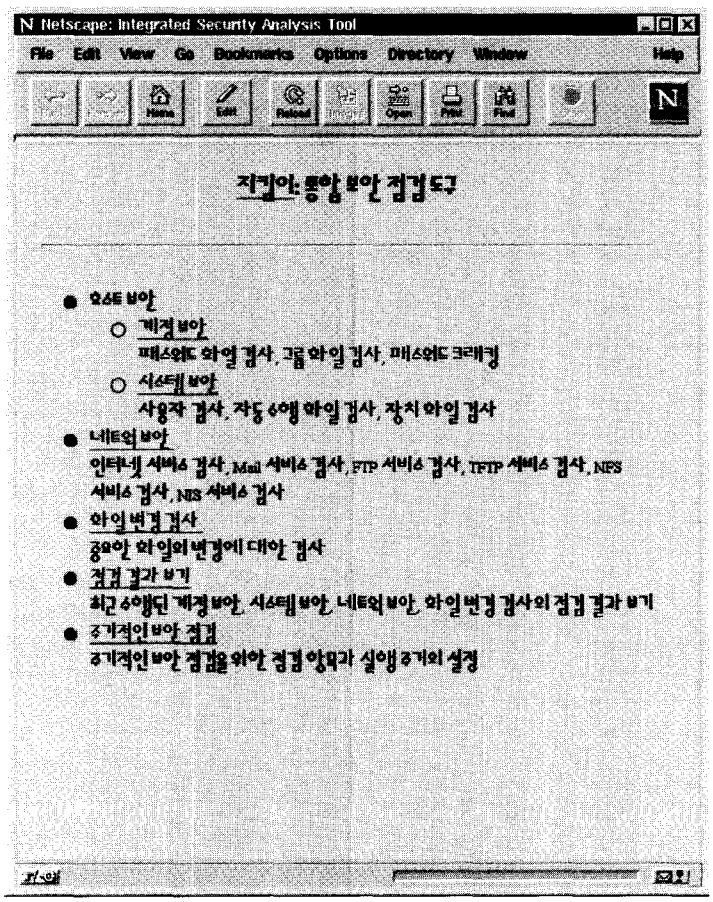


그림 1 지킴이의 첫 화면

단순한 조합이 아니라 시스템의 전반적인 보안에 대한 점검을 위하여 필수적인 기능을 제공하도록 구성되었다. 표 1은 지킴이에서 제공하는 점검 기능과 관련된 기존의 보안 도구를 나타낸 것이며, 그림 1은 구현된 지킴이의 첫 화면이다.

2.1 계정 보안

계정 보안은 시스템 보안의 가장 근본이 되는 부분으로서, 패스워드 화일과 그룹 화일에 대한 검사와, 패스워드의 안전성을 크랙을 이용하여 점검하는 기능을 제공한다.

- 패스워드 화일 검사: 패스워드 화일(**/etc/passwd**)은 시스템 사용자의 계정에 대한 정보를 저장하는 화일로서, 지정된 사용자 이름 또는 id의 유효성, 중복된 사용자 이름 또는 id의 존재 유무와, 지정된 홈 디렉토리의 존재 및 사용자의 소유 여부 등에 대한 검사를 한다. 또한, 패스워드를 지정하지 않은 사용자와 불허된(locked) 패스워드[1]를 가진 사용자에 대한 검사를 한다.

1 패스워드 필드가 '*'로 시작하는 경우로서, 시스템 관리자들이 계정의 사용을 일시적으로 금지시킬 때 일반적으로 사용하는 방법이다.

- 그룹 화일 검사 : 시스템에서 지정된 그룹에 대한 정보를 저장하는 화일(/etc/group)에 대하여, 그룹 이름 또는 id의 유효성, 중복된 그룹 이름 또는 id의 사용 등에 대한 검사를 수행한다.
- 패스워드 크래킹[1, 9] : 시스템에 대한 대부분의 침투는 취약한 패스워드를 이용하는 것부터 시작된다. 지킴이는 크래킹을 이용하여 이러한 취약한(추측되기 쉬운) 패스워드를 찾음으로써, 시스템의 계정 보안성을 향상시킬 수 있다.

패스워드 화일 검사와 그룹 화일 검사 기능은 COPS[2]에서 제공하는 기능과 유사하며, 지킴이에서는 쉐도우 패스워드 화일(shadow password file)에 대한 고려가 추가되었다. 시스템에서 쉐도우 패스워드 화일을 사용하는 경우 암호화된 패스워드가 쉐도우 패스워드 화일에 있기 때문에 패스워드가 없는 사용자와 불허된 패스워드를 가진 사용자에 대한 검사는 쉐도우 패스워드 화일에 대한 분석이 요구된다. 또한, 지정된 홈 디렉토리에 대한 사용자의 소유 여부에 대한 검사가 추가되었다.

패스워드 크래킹은 기존의 대표적인 도구인 Crack을 바탕으로 하여, 한글 단어 사전을 이용한 크래킹을 지원하도록 확장하였다. Crack은 기본적으로 유닉스 시스템에서 제공하는 영어 단어 사전(**/usr/dict/words**), 주로 사용되는 패스워드 사전, 그리고 전문 약어를 이용하여 패스워드를 추측한다. 그러나, 우리나라에서는 많은 사용자들이 한글 단어를 패스워드로 사용하는 현실이므로, 지킴이에서는 한글 단어를 이용하여 취약한 패스워드를 추측하는 기능을 제공하며, 실제로 이 기능은 지킴이를 실제 운용 중인 시스템에 적용해 본 결과 상당한 효과가 있음이 확인되었다.

표 2는 계정 보안에서 제공하는 점검 항목들이다. 각 항목에 대한 오류는 그 중요성에 따라서, 심각과 경고로 분류된다. 시스템의 무결성 또는 보안과 관련된 사항은 심각으로 분류되며 그렇지 않은 것은 경고로 분류된다. 예를 들어, 중복된 사용자 이름 또는 id의 사용과 패스워드가 없는 계정의 존재는 계정의 무결성과 보안성을 위배하는 것이므로 심각으로 분류되며, 멤버가 존재하지 않는 그룹과 불허된 패스워드의 사용은 경고로 분류된다.

점검 항목	세 부 항 목	오류 수준
패스워드 화일 검사	패스워드 화일의 필드 수	심각
	유효한 사용자 이름 및 id의 사용	심각
	유효한 그룹 id의 사용	심각
	중복된 사용자 이름 및 id의 사용	심각
	불허된 패스워드의 사용	경고
	패스워드의 존재 여부	심각
	홈 디렉토리의 존재와 소유 여부	심각
그룹 화일 검사	그룹 화일의 필드수	경고
	유효한 그룹 이름 및 id의 사용	심각
	중복된 그룹 이름 및 id의 사용	심각
패스워드 크래킹	패스워드의 추측 가능	심각

표 2 : 계정 보안의 점검 항목

2.2 시스템 보안

시스템 보안은 보안과 관련된 다양한 검사 기능을 제공하며, 표 3은 시스템 보안에서 제공하는 점검 항목들을 나타낸다.

- 사용자 검사 : 사용자와 관련된 화일 또는 설정의 적합성을 조사한다
  1. 홈 디렉토리의 world writability 검사: 각 사용자의 홈 디렉토리를 다른 사용자가 쓰는 것을 허용해서는 안 된다.
  2. 시작 화일의 검사: 홈 디렉토리에는 **.profile, .cshrc, .exrc, .rhosts** 등과 같이 '.'으로 시작하는 화일이 있다. 이 화일들은 특정 프로그램들의 구동 시 사용되는 화일로서, 프로그램의 수행에 영향을 준다. 이 시작 화일을 변경함으로써, 해당 사용자 또는 시스템 관리자의 권한이 노출되는 상황이 발생할 수가 있으므로, 타인에게 이러한 시작 화일에 대한 쓰기를 허용해서는 안 된다. 또한 **.netrc**와 같은 화일은 사용자의 이름과 패스워드가 그대로 저장되는 경우도 있으므로, 읽기도 허용해서는 안 된다. 그리고, 인증 과정을 거치지 않고 시스템에 대한 사용을 허가하는 사용자를 지정하는 화일인 **.rhosts**에 wild card('+')가 지정되어 있는 지를 검사한다. '+'는 임의의 사용자에게 시스템에 대한 권한을 주는 것이므로, 이의 사용은 금지되어야 한다. 시스템 관리자의 시작 화일들에 대해서는 더욱 엄격한 검사를 한다. 즉, 시작 화일 자체의 쓰기 권한 뿐만 아니라, 시작 화일 안에 기술된 화일에 대한 쓰기 권한에 대한 검사도 수행한다.
  3. 주요 화일의 소유자 및 사용권한 검사: 시스템에는 **/etc/passwd**와 같이, 시스템 관리자가 반드시 소유해야 하는 시스템 화일들이 있으며, 또한 이들 화일들은 시스템 관리자에 의해서만 쓰거나 읽기가 가능하다. 이 검사에서는 이러한 시스템의 주요한 화일의 시스템 관리자 소유 여부와 적절한 사용 권한이 설정되어 있는 지를 조사한다.
  4. umask 값 및 검색 경로(search path) 검사: umask 값은 생성되는 화일의 초기 사용 권한의 결정에 영향을 준다. 따라서, 사용자들 - 특히 시스템 관리자 - 이 적절한 umask 값을 설정하고 있는 지를 검사한다. 검색 경로에 지정된 경로(path)들의 world writability와, 현재 디렉토리('.')가 검색 경로에 포함되어 있는 지를 검사한다.
- 자동수행 화일 검사 : 시스템에는 **/etc/rc***의 형태로서, 시스템이 구동 또는 종료 시 자동으로 수행되는 화일들이 있다. 이러한 화일들은 구동 또는 종료 시 시스템에서 필요한 작업들을 자동으로 수행하기 위해 여러 가지 세부 작업 프로그램들을 호출한다. 또한, 사용자가 특정 프로그램의 주기적인 수행을 요구한 경우, 이 정보는 cron 테이블에 기록되며 지정된 시간에 시스템에 의해 자동적으로 수행된다. 이러한 rc화일 또는 cron 화일들은 관리자가 부주의하기 쉽고, 자주 수행이 되는 프로그램이기 때문에, 각 프로그램들이 원하는 작업만을 제대로 수행하고 있는 지에 대한 검사가 필요하다. 지킴이는 이러한 rc 화일 또는 cron 화일에 지정된 프로그램들에 대한 world writability를 검사한다.
- 장치 화일 검사 : 시스템에서 사용하는 다양한 장치 화일(device file)에 대하여 world writability와 world readability를 검사한다. NFS 서비스를 통하여 사용되는 원격 화일 시스템에 대한 검사는 네트웍 보안에서 수행된다.

점검 항목	세 부 항 목	오류 수준
사용자 검사	홈 디렉토리의 world writability 검사	심각
	시작 화일의 검사	심각
	주요 화일의 소유자 및 사용권한	심각
	umask, 검색 경로 검사	심각
자동 수행 화일 검사	rc 화일 검사	심각
	cron 화일 검사	심각
장치 화일 검사	world readagility/writability 검사	심각

표 3 : 시스템 보안의 점검 항목

시스템 보안에서 제공하는 기능들은 대부분 COPS에서도 제공된다. 지킴이는 COPS에서 제공하는 다양한 점검 항목들을 간결하고 명확하게 구성하여 관리자가 시스템의 보안에 관련된 사항들을 쉽게 이해할 수 있도록 하였다.

2.3 네트웍 보안

유닉스 시스템에서 제공하는 다양한 네트웍 서비스는 사용자들에게 편리함과 시스템 자원의 활용도를 향상시키는 역할을 한다. 그러나, 네트웍 서비스에 대한 적절한 설정이 이루어지지 않은 경우, 보안상 취약점이 노출되는 경우가 많다. 지킴이는 FTP, TFTP, NFS, NIS, Mail과 같은 시스템이 제공하는 여러 가지 네트웍 서비스에 대한 점검을 수행한다. 표 4는 시스템 보안에서 제공하는 점검 항목들을 나타낸다.

- 인터넷 서비스 검사: 유닉스 시스템에서는 **/etc/hosts.equiv** 또는 각 사용자 홈 디렉토리의 **.rhosts**화일을 이용하여 신뢰(trust)할 수 있는 호스트 및 사용자를 지정한다. 이러한 화일에 임의의 사용자를 의미하는 '+'의 사용은 금지되어야 한다. 여기에서는 **/etc/hosts.equiv** 화일에 대해서만 검사를 하며 **.rhosts** 화일에 대한 검사는 시스템 보안의 사용자 검사에서 수행된다. **/etc/inetd.conf** 화일은 제공되는 네트웍 서비스에 대한 종류 및 서버를 지정하는 화일이다. 이 화일에 지정된 서버가 시스템의 쉘과 일치하는 지를 조사하며[2], 또한, **rpc.rexd**와 같은 아무런 인증 과정이 필요 없는 서비스가 지원되고 있는지를 검사한다.
- Mail 서비스 검사: Sendmail은 인터넷에서 mail을 전송하기 위하여 많이 이용되는 프로그램으로서, 이미 많은 버그가 알려졌고, 아직도 있다고 생각되는 프로그램이다. 지킴이에서는 SMTP 포트로 연결을 시도하여 sendmail의 버전을 검사하고, debug 명령이 제공되는 지를 검사한다. 또한, decode 또는 uudecode의 alias가 있는 지를 검사한다.
- FTP(File Transfer Protocol) 서비스 검사: 일반적으로 FTP 서비스의 사용을 제안해야 하는 root, uucp, news, bin 등과 같은 계정들을 **/etc/ftpusers**에 지정하고 있는지를 검사하며, 안전한 익명 FTP 서비스를 제공하기 위한 설정이 잘 되어 있는 지를 검사한다

2 서버가 쉘과 일치하게 되면, 외부에서 시 서비스를 요청할 때 쉘이 수행되므로, 공격자에게 시스템에 대한 권한이 노출된다.

- TFTP(Trivial File Transfer Protocol) 서비스 검사: 사용자의 인증 과정이 없는 화일 전송 서비스로서, 주로 X-terminal이나 diskless 클라이언트의 구동을 위해서 사용된다. TFTP 서비스의 데몬을 실행시킬 때, secure 옵션이 설정되어 있는 지를 검사하며, 실제로 TFTP 서비스를 이용하여 화일의 유출이 가능한 지를 검사한다
- NFS(Network File System) 서비스 검사: 자기 시스템에서 이용하고자 하는 원격의 화일 시스템을 mount 테이블에 지정하며, 원격 시스템에게 제공하는 자신의 화일 시스템에 대한 설정은 export 테이블에 지정한다.

1. mount 테이블 검사: 지킴이에서는 mount 테이블에 지정된 NFS 화일 시스템에 대한 읽기/쓰기 가능성을 검사한다.
2. export 테이블 검사: 화일 시스템이 쓰기 권한을 가지고 제공되는 지, root 권한으로 제공되고 있는 지와 임의의 호스트에게 제공되고 있는 지를 검사한다.

- NIS(Network Information System) 서비스 검사: NIS 서비스는 다수의 호스트들의 중요한 시스템 화일들을 네트웍을 통해서 공유함으로써 관리자와 사용자에게 일관성 있는 시스템 환경을 제공한다. NIS 서비스는 도메인 이름(domain name)을 통해서 서비스 받을 시스템의 영역을 정하며, 도메인 이름이 쉽게 추측 가능한 것을 사용하면 보안상 큰 문제가 된다. 지킴이에서는 NIS 데몬이 secure 옵션을 사용하도록 설정되어 있는 지를 검사한다.

이러한 점검 기능을 수행하는 기존의 보안 도구로는 SATAN과 ISS가 있다. 원격 시스템에 대한 점검을 이러한 도구와는 달리, 지킴이는 관련된 화일들을 조사함으로써 네트웍 서비스가 잘 설정되어 있는 지를 검사한다. 따라서, 좀 더 정확하면서도 효과적인 검사가 이루어질 수 있으며, SATAN, ISS에서처럼 이 도구가 공격에 이용되는 부작용을 방지할 수 있다.

점검 항목	세 부 항 목	오류 수준
인터넷 서비스 검사	Trusted Host의 지정	심각
	/etc/inetd.conf의 설정	심각
Mail 서비스 검사	Sendmail의 버젼	심각
	debug 명령어의 제공	심각
	decode와 uudecode alias 사용	심각
FTP 서비스 검사	**/etc/ftpusers** 화일 설정	경고
	익명 FTP 서비스의 설정	심각
TFTP 서비스 검사	데몬의 secure 옵션 지정	심각
	읽기 가능	심각
NFS 서비스 검사	mount 테이블 설정	경고
	export 테이블 설정	심각
NIS 서비스 검사	데몬의 secure 옵션 지정	심각

표 4 : 네트웍 보안의 점검 항목

2.4 화일 변경 검사

침입자는 시스템의 root 권한을 획득하기 위해서 또는 미래의 침입을 위한 back door를 만들기 위해서, 혹은 다른 호스트로의 침입을 위해서 화일을 조작한다. 따라서, 시스템의 중요한 화일들에 대한 지속적인 점검은 필수적이다. 화일 변경 검사는 다음과 같이 수행될 수가 있다.

- 데이터베이스 초기화: 시스템을 설치한 후, 감시될 필요가 있는 중요한 화일들에 대한 자료를 수집한다. 감시될 화일들의 목록은 환경 화일(configuration file)에 지정된다. 환경 화일에는 감시될 화일의 이름 뿐만 아니라, 각 화일 별로 수집되는 자료(화일의 크기, 소유자, 사용권한, 내용, 생성/변경 날짜, . . .)가 명시된다.
- 화일 변경 검사: 환경 화일에 지정된 화일에 대한 현재의 자료를 수집하여, 이전에 수집되었던 것과 비교하여, 새로 생성된 화일, 변경된 화일, 삭제된 화일을 판단한다. 화일의 변경에서는 화일의 크기, 소유자, 사용권한 뿐만 아니라, MD5, Snefru와 같은 시그너쳐 함수를 이용하여 화일 내용 자체의 변경에 대한 검사도 수행된다.
- 검사 결과 보기 및 갱신: 화일 변경 검사 후에, 사용자는 생성, 변경, 삭제된 화일들에 대한 정보를 얻을 수 있으며, 선택적으로 새 자료를 데이터베이스에 저장할 수가 있다.

화일 변경 검사 기능은 기존의 Tripwire[5] 도구를 바탕으로 하여 화일 변경 검사에 기본적인 기능만을 제공할 수 있도록, 그리고 사용자에게 편리한 환경을 제공할 수 있도록 수정하였다.

2.5 주기적인 보안 점검

시스템 보안을 위해서는 시스템 관리자의 지속적인 관심과 관리가 필요하다. 지킴이는 WWW 브라우저를 통하여 관리자가 일일이 각 점검의 수행을 지시하는 것이 아니라, 지정된 시간에 지정된 점검을 수행하는 기능을 제공함으로써, 관리자의 편의성을 높인다. 관리자가 지킴이에서 지원하는 각 점검 항목 별로 수행 시간을 지정하면, 지킴이는 지정된 시간에 지정된 점검 프로그램을 자동으로 수행시키며, 그 결과는 관리자에게 전자우편으로 통보된다.

3. 지킴이의 구현

지킴이는 크게 두 가지 종류의 모듈로 구성된다. 인터페이스 모듈은 사용자가 원하는 점검 항목을 선택하여 보안 점검을 시작할 수 있는 WWW 화면을 제공하며, 보안 점검 모듈은 실제로 점검을 수행한다. 인터페이스 모듈은 지킴이의 초기 화면을 생성하는 최상위 인터페이스(Main Interface) 모듈과 각 범주별로 각각의 화면을 생성하는 5개의 인터페이스 모듈(Account Security Interface, System Security Interface, Network Security Interface, File Integrity Interface, Scheduler Interface)로 구성된다.

인터페이스 모듈은 WWW 브라우저를 이용한 사용자 인터페이스를 제공하기 위해서 HTML 문서를 생성하며, 각 점검 모듈은 실제 점검을 수행하는 프로그램으로서, 모두 Perl로 구현되었다. Perl은 대부분의 시스템에서 동작되는 스크립트 언어로서 높은 이식성을 제공한다. 다만, 패스워드 크래킹 모듈과 화일 변경 검사 모듈에서는 기존의 Crack 프로그램과 Tripwire 프로그램을 이용하도록 구현되었다.

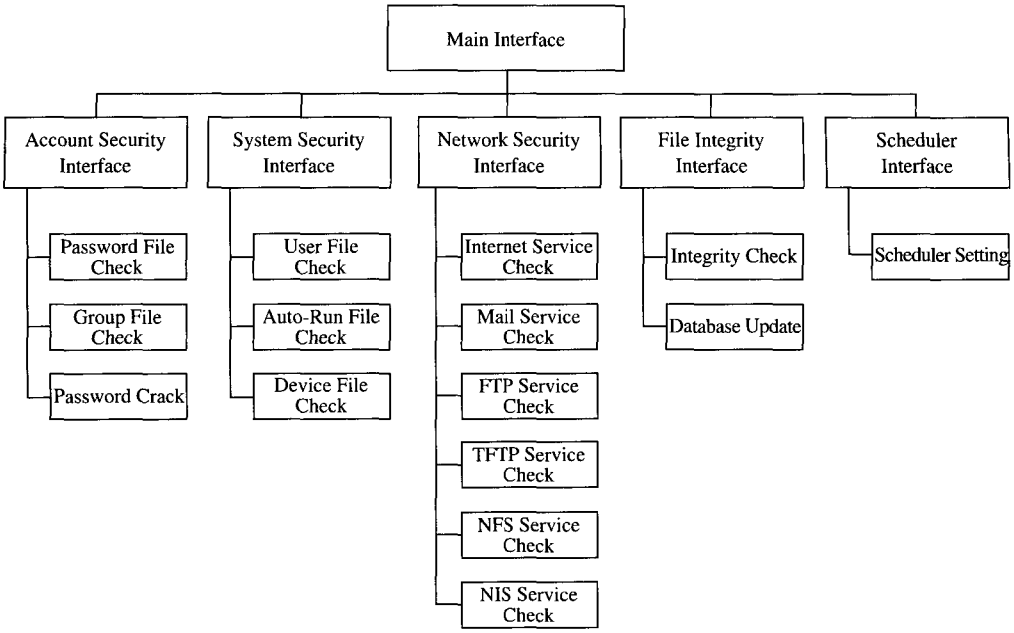


그림 2 지킴이의 구조

지킴이는 각 점검 항목별로 모듈화 하였고, Perl을 이용하여 구현하였기 때문에, 높은 이식성과 확장성을 제공한다. 지킴이의 전체적인 구조는 그림 2와 같다.

3.1 인터페이스 모듈

최상의 인터페이스 모듈은 SATAN의 수행 방식을 응용하여 구현하였다. 모듈은 기본적인 클라이언트/서버 프로그램 방식의 응용으로, 클라이언트 프로세스는 WWW 브라우저를 실행시켜서 사용자의 입력을 받아들이고, 서버 프로세스에게 지정된 네트웍 포트를 통해서 사용자의 요구를 전달한다. 전달된 사용자의 요구를 분석한 서버 프로세스는 해당 보안 점검 모듈을 호출하여 점검을 수행하게 하고, 수행된 결과 화일을 읽어서 HTML 형식의 문서를 만들고, 클라이언트 프로세스의 WWW 브라우저 상에 문서를 쓴다.

또한, 점검 결과의 Hyper-link를 따라가면 문제에 대한 자세한 설명과 간단한 해결책을 HTML 문서로 제공하도록 구현하였다. 보안에 관한 전문적인 지식이 없는 관리자라도 쉽게 이해할 수 있을 정도의 문서를 제공한다. 예를 들어, 그림 3은 패스워드 크래킹에 관한 Hyper-link를 따라 갔을 때 보여지는 도움말 화면이다.

3.2 계정 보안 점검 모듈

패스워드 화일 검사 모듈과 그룹 화일 검사 모듈은 COPS를 바탕으로 하여 구현하였다. 패스워드 크래킹 모듈은 Crack의 기능을 바탕으로 하여, 한글 사전[3]을 이용한 크래킹을 지원하도록 구현하였다. 한글 사전을 이용하여 크래킹을 수행하는 과정은 다음과 같다.

3 한글 사전은 한국과학기술원 전산학과 최기선 교수 연구실에서 제작한, 50000 여개의 명사로 구성된 사전을 이용하였다. 이 사전은 공개된 것이 아니며, 연구용으로만 사용하기로 최기선 교수 연구실과 협약을 맺었다.

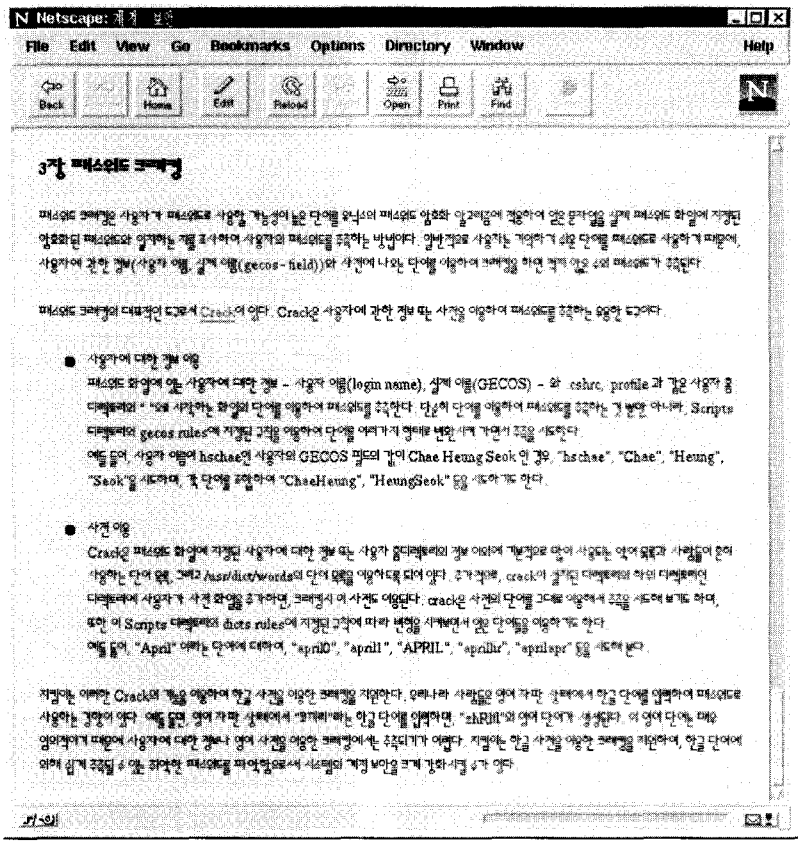


그림 3 패스워드 크래킹에 대한 도움말

1. 완성형 한글을 조합형으로 변환한다.
2. 한글 2벌식 자판과 영어 자판 사이의 관계를 이용하여, 조합형 한글 단어를 해당하는 영어 단어로 변환한다. 예를 들면, 한글 2벌식 자판에서 '가'는 영어 자판의 'rk'에 해당한다. 이를 위해서는 먼저, 한글 단어의 각 음절에서 초성, 중성, 종성 부분을 추출하고, 이를 영어 자판의 해당하는 알파벳으로 변환하는 작업이 필요하다.
3. 크래킹을 수행한다.
4. 크래킹에서 추측된 패스워드를 원래의 한글 단어로 변환하여 보여준다.

3.3 시스템 보안 점검 모듈

시스템 보안 점검 모듈은 사용자 검사, 자동 수행 화일 검사, 장치화일 검사를 수행하며, COPS에서 제공하고 있는 기능을 바탕으로 한다. 단, 기존의 COPS 프로그램보다 가독성과 이식성을 높이는 것에 중점을 두고 구현하였다.

3.4 네트워 보안 점검 모듈

SATAN과 같은 기존의 네트워 보안 점검 도구는 관리자에게 유용한 정보를 제공하지만, 반면에 악의를 가진 외부인에게도 같은 양의

정보를 제공하는 역기능도 있다. 따라서, 지킴이는 이러한 점을 해결하기 위해서 보안 점검 대상을 도구를 사용하는 시스템 내의 네트웍 서비스 설정에 대한 점검으로만 제한하여 구현되었다. 개발된 지킴이의 네트웍 보안 점검 모듈은 기존의 보안 점검 도구와 같은 정도의 정보를 제공하면서, 역기능이 없고, 새로운 네트웍 보안 점검 모듈의 추가가 용이하다.

3.5 화일 변경 검사 모듈

화일 변경 검사 모듈은 Tripwire의 기능을 이용하여, 편리한 사용자 인터페이스를 제공하도록 구현하였다. Tripwire는 화일 변경 검사 기능을 제공하는 강력한 도구이지만, 사용자 인터페이스가 불편하며, 필요 이상의 기능을 제공하는 면도 있다. 지킴이는 화일 변경 검사의 필수적인 기능 - 데이터베이스 구축, 화일 변경 검사, 검사 결과 보기 및 갱신 - 을 편리한 사용자 인터페이스와 함께 제공한다. 즉, 사용자는 동일한 인터페이스로 주요한 세가지 기능을 수행시킬 수 있으며, 화일 변경 검사를 수행한 결과를 WWW 브라우저를 이용하여 일목요연하게 분석할 수 있다. 또한, 변경된 화일들에 대한 자료를 데이터베이스에 갱신하는 과정도 쉽게 할 수 있다. 예를 들어, 그림 4는 변경된 화일에 대한 자세한 정보를 보여주는 화면이다. 사용자는 화일의 변경 사항의 하단의 체크 박스를 선택함으로써 해당 화일에 대한 데이터베이스의 갱신을 요구할 수 있다.

3.6 주기적인 보안 점검 모듈

앞에서 설명된 여러 점검 모듈들의 주기적인 점검 시간을 사용자가 쉽게 지정할 수 있도록 radio button 방식의 사용자 인터페이스를 제공한다. 사용자가 지정한 점검 항목에 해당하는 점검 모듈을 지정된 시간에 자동적으로 수행시키도록 root의 cron 테이블에 추가한다.

4. 적용 사례

이 절에서는 지킴이를 실제 운용 중인 시스템에 시험 적용한 결과를 알아보겠다. 시험 대상 시스템은 한국과학기술원 전산학과 학생들이 사용하는 학과의 시스템으로 운영체제는 SunOS 4.1.3-KL이고, 사용자수는 600 여 명이다. 이 시스템은 NIS 클라이언트이고, NFS 클라이언트이면서 NFS 서버로 사용되며, 5명의 관리자가 있어서 비교적 관리가 잘 되고 있다고 알려져 있다. 계정 보안, 시스템 보안, 네트웍 보안의 점검 결과는 표 5와 같다.

● 계정 보안

패스워드 화일의 필드 수는 7이어야 하는데, 대상 시스템의 8개의 계정이 쉘 부분을 지정하고 있지 않았고, 대상 시스템에는 2개의 계정이 중복된 id를 가지고 있었는데, 이 두 계정은 서로 상대방의 화일에 대한 권한을 가지게 되므로 보안상 문제가 된다. 불허된 패스워드를 사용하는 19개의 계정이 있었는데, 이것은 임시로 사용자의 계정을 삭제할 때, 패스워드 필드의 앞에 '*'를 넣은 것으로 보안상 문제는 없다. 또한, 대문자로 된 사용자 이름을 가지는 계정과 8문자 이상의 길이를 가지는 계정이 각각 하나씩 있었는데, 확인 결과 보안상 문제는 없었다. 그리고, 지정된 홈 디렉토리가 없거나, 소유자가 다른 계정이 11개가 발견되었으며, 멤버가 지정되지 않은 그룹이 20개 발견되었다. 이러한 오류들은 수백 명의 사용자를 관리해야 하는 시스템 관리자의 부주의에 의한 것이다.

패스워드 크래킹의 결과 총 62개의 계정의 패스워드를 추측하였으며, 사전의 종류별로

범 주	점검 항목	세 부 항 목	오류 수
계 정 보 안	패스워드 화일 검사	패스워드 화일의 필드 수	8
		유효한 사용자 이름 및 id의 사용	2
		유효한 그룹 id의 사용	0
		중복된 사용자 이름 및 id의 사용	2
		불허된 패스워드의 사용	19
		패스워드의 존재 여부	0
		홈 디렉토리의 존재와 소유 여부	11
	그룹 화일 검사	그룹 화일의 필드 수	20
		유효한 그룹 이름 및 id의 사용	0
		중복된 그룹 이름 및 id의 사용	1
	패스워드 크래킹	패스워드의 추측 가능	62
시스템 보 안	사용자 검사	홈 디렉토리의 world writability	0
		시작 화일의 검사	5
		주요 화일의 소유자 및 사용권한	0
		umask, 검색 경로 검사	0
	자동 수행 화일 검사	rd 화일 검사	5
		cron 화일 검사	0
	장치 화일 검사	world readability/writability	0
네트웍 보 안	인터넷 서비스 검사	Trusted Host의 지정	0
		/etc/inetd.conf의 설정	0
	Mail 서비스 검사	Sendmail의 버젼	0
		debug 명령어의 제공	0
		decode와 uudecode alias 사용	0
	FTP 서비스 검사	/etc/ftpusers 화일 설정	1
		익명 FTP 서비스의 설정	0
	TRTP 서비스 검사	데몬의 secure 옵션 지정	0
		읽기 가능	0
	NFS 서비스 검사	mount 테이블 설정	0
		export 테이블 설정	0
	NIS 서비스 검사	데몬의 secure 옵션 지정	1

표 5 :점검 결과 - 계정 보안, 시스템 보안, 네트웍 보안

나누어보면, 사용자에 대한 정보만을 이용하였을 때는 10개, Crack에서 제공하는 사전만을 이용하였을 때 27개, 지킴이에서 추가한 한글 사전만을 이용하였을 때 25개를 추측하였다. 이러한 결과를 보면, 지킴이의 한글을 사용하는 크래킹은 우리나라의 실정

에서 상당히 효과적임을 알 수 있다. 이 크래킹을 통해 추측된 패스워드의 수는 대상 시스템 사용자의 약 10%에 해당하는 것으로, 아직도 많은 사용자들이 추측이 어려운 패스워드 사용하여야 한다는 보안의 기초적인 사항을 잘 지키지 않음을 알 수 있다.

● 시스템 보안

시스템 보안의 점검 결과에서 root의 시작 화일 **.cshrc**에 포함된 5개의 화일이 world writable하게 지정되어 있다. Oracle의 두개의 실행 화일 - coraenv와 oraenv - 이 world writable이었지만, 스크립트가 아니라 binary이므로 보안상 큰 문제는 없는 것으로 확인되었다. **/etc/hosts.equiv**가 world writable이라서 심각한 문제인 것처럼 보이지만, 실제로 살펴보면 **/dev/null**로 링크가 되어 있었다. 현재 mount 된 화일 시스템을 보여 주는 **/etc/mtab**이 world writable인 것은 관리자의 소홀이며, 보안상 문제는 초래하지 않는다.

자동 수행 화일 중 rc 화일에 지정된 5개의 화일이 world writable하게 지정되어 있었는데, 4개는 확인 결과 문제가 없는 것이었지만, **/var/spool/mqueue** 디렉토리는 문제의 소지가 있다. 이 디렉토리는 전송될 전자우편이 임시로 저장되는 장소로, world writable하게 지정되어 있으면 다른 사용자의 메일 내용을 임의로 변경하거나 삭제할 수 있게 된다.

● 네트웍 보안

네트웍 보안의 점검 결과, 대부분의 네트웍 서비스가 안전하게 제공되고 있음을 알 수 있었다. 대상 시스템은 **/etc/ftpusers** 화일이 없는데, 이 화일은 root와 같은 시스템 계정을 이용한 FTP 서비스를 제한하기 위한 것으로 보안상 치명적인 문제는 아니지만, 좀 더 안전한 FTP 서비스를 위해서 권장된다. 또한, 대상 시스템은 NIS secondary server로 지정된 시스템으로 NIS 데몬이 secure 옵션 없이 사용되고 있는데, secure 옵션을 설정하면 좀 더 안전한 서비스를 제공하지만, 없어도 보안상 문제는 초래하지 않는다.

대부분의 네트웍 서비스들은 다른 보안 항목과는 달리 자주 변경되는 부분이 아니다. 따라서, 시스템 최초의 설정대로 사용하거나, 지킴이에서 검사하는 사항들에 주의하면서 서비스 설정을 한다면 안전한 서비스를 제공할 수 있다.

● 화일 변경 검사

검사된 화일의 총 개수	생 성	삭 제	변 경
4267	41	19	153

표 6 점검 결과: 화일 변경 검사

표 6은 대상 시스템에서 화일 변경 검사를 7일간에 걸쳐 수행한 결과이며, 그림 4는 변경된 화일들에 대한 정보를 나타내는 화면의 일부이다. 시스템 관리자는 그림 4와 같은 결과를 분석하여 '불법적인 변조' 있는지를 확인하는 작업을 해야 한다. 대상 시스템에는 시스템 관리자가 5명이었기 때문에, 일관성 있는 화일 관리가 이루어지지 않아 화일 변경에 대한 확인이 어려웠으나, 담당 시스템 관리자들의 협조로 변경 사항을 확인한 결과, 화일의 불법적인 변조나 침투 흔적은 없다는 결론을 내릴 수 있었다. 지킴이에서는 구현되지 않았지만, 화일 변경 검사 결과로부터 수작업이 아니라, 화일 변경의 내용을 분석하여 자동적으로 침입의 흔적을 찾는 도구도 필요하겠다.

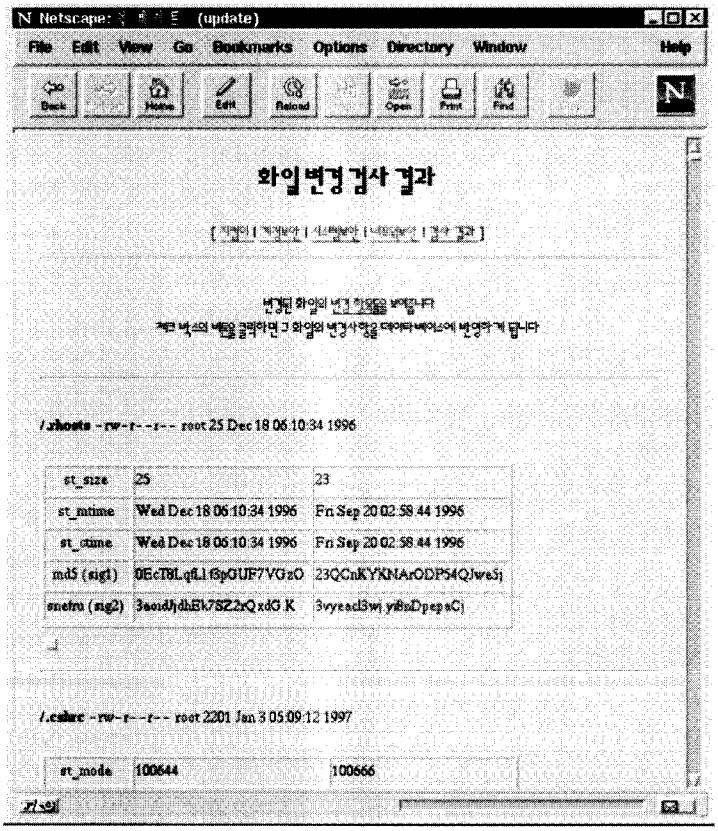


그림 4 점검 결과: 화일 변경 검사

5. 결론 및 향후 연구 방향

편리한 사용자 인터페이스와 다양한 부분에 대한 점검 기능은 시스템의 보안에 대한 지속적이면서 효율적인 관리를 위해서 보안 도구는 필수적으로 제공해야 한다. 본 논문에서는 시스템의 전반적인 점검 기능과 편리한 사용자 인터페이스를 제공하는 통합 보안 점검 도구 - 지킴이 - 를 제안하고, 구현하였으며 지킴이를 실제 운용 중인 시스템에 적용하여 본 결과, 보안상 중요한 결함을 포함한, 시스템의 많은 문제를 효과적으로 발견할 수 있었다.

지킴이는 보안의 기본적인 부분인 계정 보안, 시스템 보안, 네트웍 보안, 그리고 화일 변경 검사 기능을 제공하며, 관리자의 효율적인 점검을 돕기 위하여 주기적인 보안 점검 기능을 제공한다. 또한, 점검 항목과 발견된 문제에 대한 설명, 그리고 대처 방법을 사용자에게 온라인으로 제공함으로써 시스템에서 발견된 문제를 정확하게 인식할 수 있고, 효과적인 대책을 세울 수 있도록 한다.

지킴이는 각 점검 항목 별로 모듈화 되게 설계 되었으며, 구현 언어로 Perl을 사용하기 때문에, 높은 확장성과 이식성을 제공한다. 즉, 새로운 점검 항목의 추가 또는 점검 항목의 변경이 용이하므로, 도구의 기능 확장 및 개선이 수월하다.

지킴이를 개발하고 실제 시스템에 적용해

본 결과, 몇 가지 면에서 지킴이를 개선 또는 확장 시킬 수 있다고 판단된다. 먼저 계정 보안에서 패스워드 화일/쉐도우 패스워드 화일과 그룹 화일 사이의 일관성에 대한 검사가 필요하다. 패스워드 화일과 그룹 화일은 각각 사용자의 계정, 그룹에 대한 정보를 가지고 있으므로 독립적인 정보를 가지고 있는 것 같지만, 그들 사이에는 반드시 만족해야 할 연관성이 있다. 예를 들면, 그룹 화일에 그룹에 지정된 사용자는 반드시 패스워드 화일에 존재해야 한다. 또한, 패스워드 크래킹을 할 때, 패스워드 화일의 GECOS 필드에 지정된 한글 이름을 이용할 수도 있다. 즉, GECOS 필드에 영어로 지정된 사용자의 실제 이름을 한글로 변환하여, 이를 패스워드 추측에 이용할 수 있다. 예를 들어, 어떤 사용자의 GECOS 필드가 "Hong Kil Dong" 이면 "홍길동", "길동홍", "길동" 등의 단어로 크래킹을 시도해 볼 수 있다. NIS 서비스 검사에서는 크래킹을 이용하여 추측이 쉬운 NIS 도메인 이름을 파악하는 것이 추가될 수 있다. 즉, 마치 사전의 단어를 이용하여 패스워드를 다양한 방법으로 추측하는 것처럼, NIS 도메인 이름에 대해서도 사전의 단어와 다양한 규칙을 이용하여 시도할 수 있다. 화일 변경 검사에서는 변경된 화일을 분석하여 침입에 대한 판단을 돕는 기능이 추가될 수 있다. 그리고, 발견된 문제에 대한 자동적인 대처 방법도 제공할 수 있다. 예를 들어, 패스워드 화일을 검사하여 패스워드가 없는 사용자가 발견되면, 패스워드 화일을 자동으로 편집해서 이 사용자의 시스템에 대한 사용을 금지시킬 수 있다. 또한, 발견된 각 문제에 대한 몇 가지 대처 방법을 사용자에게 제시하고 사용자가 선택할 수 있는 좀 더 유연한 방법도 제공할 수 있다.

참 고 문 헌

[1] Alvare, A., "How Crackers Crack Passwords or What Passwords to Avoid," Proceedings, UNIX Security Workshop II, August 1990.

[2] Farmer, D., and Spafford, "The COPS Security Checker System," Proceedings, USENIX Conference, 1990.

[3] Farmer, D., and Venema, W., "Improving the Security of Your Site by Breaking into It," ftp://ftp.win.tue.nl/pub/security/admin-guide-to-cracking.101.Z, 1993.

[4] AUSCERT, Australian Computer Emergency Response Team, "UNIX Computer Security Checklist," 1995.

[5] Kim, G., and Spafford, E, "The Design and Implementation of Tripwire: A File System Integrity Checker," Technical Report CSD-TR-93-071, Purdue University, 1993.

[6] Curry, D., "UNIX System Security," Addison-Wesley, 1992.

[7] Denning, P., "Computers Under Attack: Intruders, Worms and Viruses," Addison - Wesley, 1990.

[8] Parker, D., "Computer Crime: Criminal Justice Resource Manual," National Institutes of Justice, 1989.

[9] Klein, D., "Foiling the Cracker: A Survey of, and Improvements to, Password Security," Proceedings, UNIX Security Workshop II, August, 1990.

[10] Russel, D., and Gangemi, G., "Computer Security Basics," O'Reilly & Associates, 1991.

[11] Garfinkel, S. and Spafford, G., "Practical UNIX Security," O'Reilly & Associates, 1991.

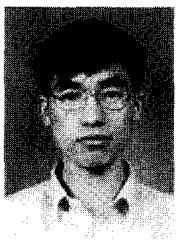
[12] Safford, D., Schales, D., and Hess, D., "The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment," Proceedings, UNIX Security Symposium IV, October 1993.

□ 著者紹介

채 홍 석

1994년 2월 서울대학교 원자핵공학과 졸업 (학사)
1996년 2월 한국과학기술원 전산학과 졸업 (공학석사)
1996년 3월 ~ 현재 한국과학기술원 전산학과 박사과정

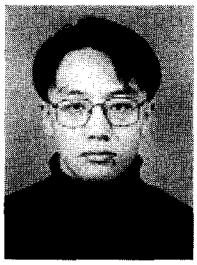
※ 주관심 분야: 소프트웨어공학, 객체지향 방법론



이 남 희

1991 년 2월 한국과학기술원 전산학과 졸업 (학사)
1994년 ~ 1995년 (주) LG 전자 미디어통신 연구소(연구원)
1996년 3월 ~ 현재 한국과학기술원 전산학과 석사과정

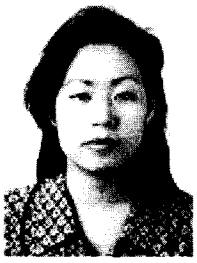
※주관심 분야: 소프트웨어공학, 실시간 시스템 명세 및 검증



김 형 호

1996년 2월 서강대학교 전자계산학과 졸업 (학사)
1996년 3월 ~ 현재 한국과학기술원 전산학과 석사과정

※ 주관심 분야: 소프트웨어공학, 객체지향 방법론



김 내 희

1996년 2월 이화여자대학교 전자계산학과 졸업 (학사)
1996년 3월 ~ 현재 한국과학기술원 전산학과 석사과정

※ 주관심 분야: 소프트웨어공학, 병렬 프로그램의 테스팅과 검증, 정형적 명세 방법론, 시스템 보안

차 성 덕

1983년 University of California, Irvine 전산학 학사
1986년 UCI 석사
1991년 UCI 전산학 박사
1990년 ~ 1991년 Hughs Aircraft Co. 연구원
1991년 ~ 1994년 The Aerospace Corp. 연구원
1994년 9월 ~ 현재 한국과학기술원 조교수

백 석 철
임 규 건
박 승 민
정 종 윤