사이버위협 관리를 위한 인터넷 위협 및 취약점 정보 수집기 설계 및 구현

이은영* · 백승현* · 박인성* · 윤주범* · 오형근* · 이도훈*

요 약

초창기 보안은 침입차단시스템에 국한되었지만 현재에는 안티바이러스, 침입 탐지 및 방화벽과 같은 관련 정보보안 솔루션들이 많아지면서 이기종의 정보보안제품들의 효율적인 관리를 위한 통합보안관리시스템이 개발·운영되고 있다. 최근에는 통합보안관리체계를 넘어서서 웜·바이러스 해킹 등 아직 일어나지 않는 사이버 위협을 관리해 능동적으로 방어할 수 있는 위협관리시스템이 보안업계의 새로운 관심분야로 떠오르고 있다. 이러한 정보보호제품의 변화에 따라 수집정보도 다양화되어가고 있으며 사이버 위협을 관리하기 위해서는 과거의 정보보안제품들로부터의 수집되는 정량적인 이벤트 로그들뿐 아니라 Microsoft, linux, 오라클과 같은 범용 어플리케이션들의 취약점 정보, 웜·바이러스 등의 악성 코드 정보, 또한 국제적 분쟁으로 인한 사이버징후와 같은 보안 뉴스들의 정성적인 정보가 필요하다. 본 논문에서는 사이버위협 관리를 위한 정보수집의 일환으로 정량적인 정보와 정성적인 정보를 수집하는 인터넷 위협 및 취약점 정보 자동수집기를 설계, 구현하였다. 제안된 수집기는 사이버위협을 관리하는데 있어 정량적인 정보 뿐 아니라 정성적인 정보를 함께 수집함으로써 사이버위협 판단의 정확성을 높이고 아직 발생하지 않은 사이버 위협에 사전에 대응하기 위한 정보로 이용될 수 있다.

Design and Implementation of Internet Threats and Vulnerabilities Auto Collector for Cyber Threats Management

Eun Young Lee* · Seung Hyun Paek* · In Sung Park*
Joo-Beom Yun* · Hung Geun Oh* · Do-Hoon Lee*

ABSTRACT

Beginning flag security it was limited in Firewall but currently many information security solutions like Anti-virus, IDS, Firewall are come to be many. For efficiently managing different kinds of information security products ESM (Enterprise Security management) are developed and operated. Recently over the integrated security management system, TMS (Threat Management System) is rising in new area of interest. It follows in change of like this information security product and also collection information is being turning out diversification. For managing cyber threats, we have to analysis qualitative information (like vulnerabilities and malware codes, security news) as well as the quantity event logs which are from information security products of past. Information Threats and Vulnerability Auto Collector raises the accuracy of cyber threat judgement and can be utilized to respond the cyber threat which does not occur still by gathering qualitative information as well as quantity information.

Key words : Internet Information Collection, Network Traffic Information Collection

* 국가보안기술연구소

1. 서 론

인터넷을 비롯한 정보통신기술의 발전으로 개인에서부터 민간 기업 및 공공기관까지 정보통신기술에 대한 의존도가 날로 심화됨에 따라 사회 주요 시설에 존재하는 취약성을 이용한 전자적 침해와 사이버 위협에 대한 위험도가 증가하고 있다.

초창기 보안은 침입차단시스템에 국한되었지만 현재에는 안티바이러스, 침입 탐지 및 방화벽과 같은 관련 정보보안 솔루션들이 많아지면서 이기종의 정보보안제품들의 효율적인 관리를 위한 ESM (Enterprise Security Management) 개념의 통합보안관리시스템이 개발 운영 되었다. ESM은 보안관리를 전사적인 차원에서 일괄된 정책을 가지고 통합적으로 관제 및 운영/관리함으로써 보안관리의 업무 효율성과 보안성 향상을 극대화 시킬 목적으로 사용되는 통합 보안관리 체계이다. 최근에는 통합 보안관리체계를 넘어서서 웜 · 바이러스 해킹 등 아직 일어나지 않는 사이버 위협을 예측해 능동적으로 방어할 수 있는 위협관리시스템이 보안업계의 새로운 관심분야로 떠오르고 있다[7].

이러한 정보보호제품의 변화에 따라 수집정보도 다양화되어가고 있으며 과거의 정보보안제품들로부터의 이벤트 로그들뿐 아니라 Microsoft, linux, 오라클과 같은 범용 어플리케이션들의 취약점 정보나 웜 · 바이러스 등의 악성 코드 정보, 또한 국제적 분쟁으로 인한 사이버징후와 같은 보안 뉴스들도 사이버 위협을 관리하는데 필요하다.

본 논문에서는 사이버 위협관리에 필요한 수집정보의 다양화를 제공하기 위해 네트워크로 부터는 트래픽 분석에 필요한 정량적인 정보를 수집하고 인터넷으로부터는 취약점 및 보안동향과 같은 정성적인 정보를 수집하는 인터넷 위협 및 취약점 정보 자동수집기를 설계, 구현하고자 한다.

본 논문의 구성은 2장에서는 네트워크 트래픽으로부터의 수집되는 정량적인 트래픽 정보 에 대해 논하고 3장에서는 인터넷 사이트로부터 수집되는 정성적인 정보수집 내용에 대해 살펴 본 후 4장에서는 인터넷 위협 및 취약점 자동 수집기의 설계 및 구현을 기술한다. 끝으로 5장에서는 결론 및 향후연구를 제시한다.

2. 네트워크 트래픽으로부터의 정량적인 트래픽 정보 수집 내용

네트워크 규모가 커지면서 기존의 시그너쳐를 이용한 공격의 탐지는 탐색할 트래픽 양이 많아지면서 침입탐지시스템의 과부하를 초래하였다. 이에 따라 네트워크 트래픽 특성을 분석하여 DoS나 인터넷 웜과 같은 네트워크 공격을 탐지하기 위한 분야들이 새롭게 연구되고 있다.

네트워크 용량 및 성능 관리 차원에서 연구되어 온 트래픽 특성 분석 기술은 패킷의 수나 바이트 크기의 양적변화 측면의 통계 데이터를 이용하는 방법에서 연구되어 왔으나 미미한 양적 변화를 일으키는 공격이나 정상적인 트래픽 과다현상에 따른 오탐률 증가로 탐지에 어려움이 있다[1].

최근에는 동일한 패킷의 흐름을 flow로 정의하고 수집한 flow들로부터 공격에 따른 트래픽 특성을 분석하여 공격을 탐지하는 방법들이 연구되고 있다[2, 4, 5].

본 논문에서 구현한 인터넷 위협 및 취약점 자동 수집기는 네트워크 트래픽으로부터 네트워크 트래픽으로부터 탐지한 침입탐지 이벤트와 시간별, Port별 프로토콜별 트래픽의 변화를 나타낼 수 있는 각종 트래픽 통계 정보 그리고 네트워크 트래픽 특성 분석에 이용할 수 있는 flow정보와 같은 정량적인 정보를 수집한다[3].

3. 인터넷 사이트로부터의 정성적인 정보 수집 내용

현재 사이버위협들로 정보통신기술 인프라 및 서비스를 보호하기위해 대부분의 업체 및 공공기관들은 여러 정보보호시스템을 도입하고 사용하고 있다. 과거의 정보보호시스템들은 침입탐지, 침입차단 시스템에서 발생되는 정량적인 정보를 이용하였다. 그러나 이러한 정량적인 정보들은 현 상황만을 나타내어 줄 뿐 사이버위협에 미리 대처하기에는 한계가 있다.

이에 최근에는 정량적인 정보 뿐 아니라 인터넷으로부터의 취약점, 악성 코드, 취신 보안뉴스와 같은 정성적인 정보를 수집하여 사이버위협의 대응에 이용하는 정보보호시스템들이 도입되고 사용되고 있다.

한 예로, Symantec에서는 전 세계에 펴져있는 자신들의 수집에이전트를 통해 위협정보를 수집하고 DeepSight라는 TMS(Threat Management System) 서비스를 제공하고 있다[7].

각종 취약점 정보와 신종 웜·바이러스 같은 악성코드들의 정보들은 여러 웹 사이트에 공지되고 있으나 이를 정보보안 관리자들이 매일 방문하여 점검하기는 쉽지 않다.

이러한 관리적인 어려움을 줄이고 사이버 위협 관리에 필요한 정보 수집을 위해 웹 자원 검색에 많이 이용되고 있는 웹 로봇 형식의 자동 수집 시스템이 필요하다.

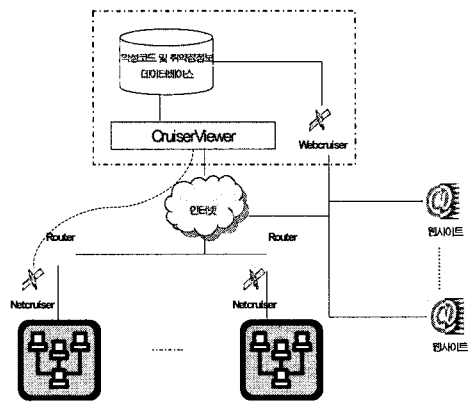
본 논문에서 구현한 인터넷 위협 및 취약점 자동 수집기는 등록된 웹사이트로부터 정보를 스케줄에 따라 자동으로 수집해 오는 시스템으로 인터넷 위협 관리에 이용될 수 있는 정성적인 정보로는 Symantec, 하우리, KrCert와 같은 정보보안서비스를 제공하는 업체로부터 수집한 경보현황과, 각종 보안 취약점, 악성 코드, 그리고 보안 뉴스를 포함한다[8-10].

4. 인터넷 위협 및 취약점 정보 자동수집기의 설계 및 구현

인터넷 위협 및 취약점 정보 수집시스템은 네트워크 트래픽을 분석함으로써 위협정보를 수집하는 NetCruiser와 인터넷 사이트로부터 위협 정보를 수집하는 WebCruiser 그리고 이들로부터 수집한 정보들을 보여주는 CruiserViewer로 이루어진다.

NetCruiser는 네트워크를 흐르는 패킷들을 분석하여 패킷 헤더에 의한 각종 네트워크 흐름에 대한 통계정보와 특징을 추출하고 이로부터 네트워크 위협을 탐지하는 네트워크 정보 수집 에이전트이다. WebCruiser는 사용자에 의해 사전 설정된 악성코드 및 취약점 정보 수집 정책에 따라 해당 웹사이트를 검색하면서 설정된 수집정보가 있을 경우 해당정보를 수집해 오는 웹 로봇 개념의 에이전트이다. CruiserViewer는 NetCruiser 및 WebCruiser로부터 수집된 정보들을 보여주는 사용자 인터페이스이다.

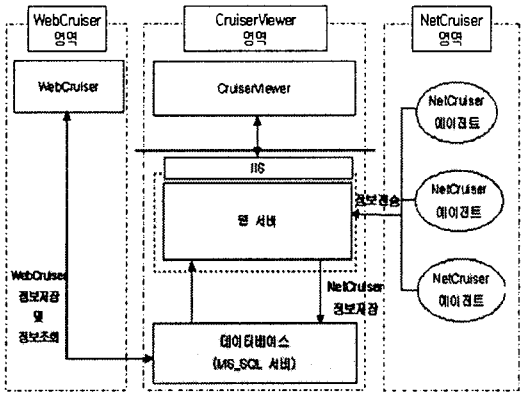
(그림 1)은 인터넷 위협 및 취약점 정보 자동수집기의 개념도이다.



(그림 1) 인터넷 위협 및 취약점 정보 자동 수집기 개념도

전체 시스템을 구성하는 서버군은 (그림 2)에서

와 같이 웹서버로 이루어진 IIS 서버, 데이터베이스 서버인 MSSQL 서버로 구성된다.



(그림 2) 전체 시스템 운영방식

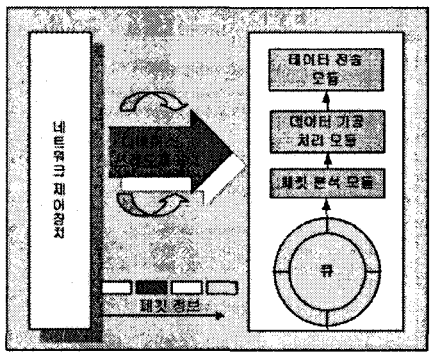
CruiserViewer는 WebCruiser와 NetCruiser에서 수집한 정보를 데이터베이스로부터 가져와서 웹페이지로 정보를 보여준다. WebCruiser는 수집할 사이트와 정책을 설정해주고 각 설정에 따라 해당 웹사이트로부터 필요한 정보를 수집하여 데이터베이스에 저장한다. NetCruiser는 해당 네트워크의 안쪽에 위치하여 네트워크 트래픽의 패킷 헤더로부터 각종 네트워크 흐름에 대한 통계정보와 flow 정보 등의 특징을 추출하여 전송한다.

4.1 NetCruiser 제작

NetCruiser는 해당 네트워크의 트래픽을 미러링하여 볼 수 있는 위치에 설치되어 네트워크 트래픽의 정량적인 정보를 수집한다.

수집되는 내용은 2장에서 기술한 바와 같이 각종 침입탐지 이벤트, 트래픽 통계정보, 패킷 헤더를 이용한 flow 정보들 이다. 각 수집 항목별로 사용자의 추가/삭제가 가능하도록 모듈별로 설계되어 필요한 정보들의 업데이트가 가능하다.

(그림 3)은 NetCruiser의 구조이다. IN, OUT의 NIC로부터 들어오는 패킷들을 쓰레드로 제어하여 패킷 저장고인 큐에 저장한다. 패킷 분석 모듈은 큐로부터 패킷을 가져와 분석하여 각 저장 구조체로 변환한다. 데이터 가공 및 처리모듈은 분석된 데이터를 수집형태에 맞게 가공하고 데이터전송 모듈은 가공된 정보들을 CruiserViewer 에게 전송한다.



(그림 3) NetCruiser 구조

NetCruiser 수집 항목은 <표 1>에서와 같다.

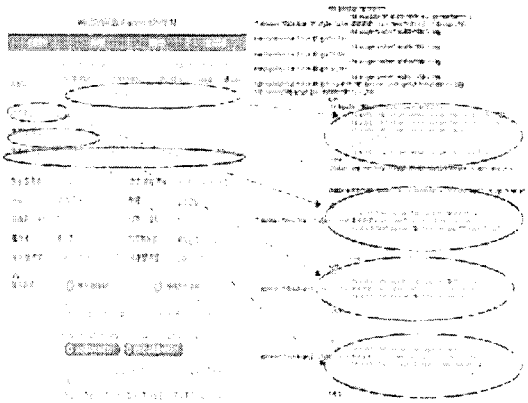
〈표 1〉 NetCruiser 수집 항목

수집항목	설 명
탐지 이벤트	네트워크 트래픽 패킷헤더를 분석하여 특정 logic 공격들의 탐지 이벤트
트래픽 통계 정 보	- 시간대별 트래픽 수/양 - Port 별 트래픽 수/양 - Protocol별 트래픽 수/양
트래픽 flow 정 보	동일한 트래픽 정보를 지닌 패킷들의 흐름정보(근원지 IP, 근원지 Port, 목적지 IP, 목적지 Port)

4.2 WebCruiser 제작

WebCruiser의 웹 사이트 정보 자동수집의 방법은 사용자가 등록한 사이트들을 대상으로 (그림 4)에서 보는 바와 같이 HTML의 형식을 사전에 분석하는 변환 플러그를 통해 사이트들의 구조를

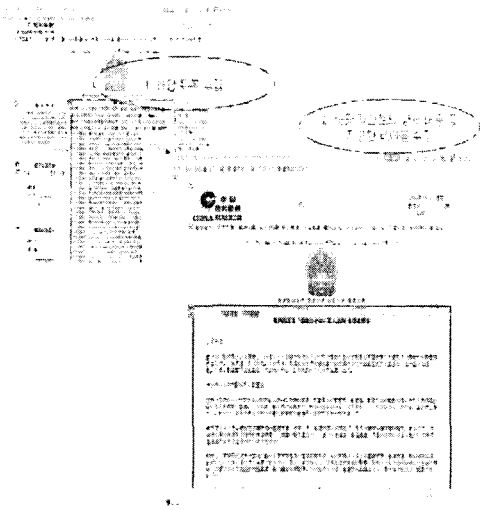
분석한 후 아래와 같은 형식의 수집항목들을 수집한다[6].



(그림 4) HTML 구조 분석

• 일반 게시판 형태의 웹사이트

해당 대상 사이트의 수집 정보에 대한 HTML 형식을 사전에 분석하는 변환 플러그-인을 통해 분석된 구조를 통해 사용자가 수집 부분을 테이블 단위로 선택하고 스케줄에 따라 선택된 테이블의 내용을 수집한다.



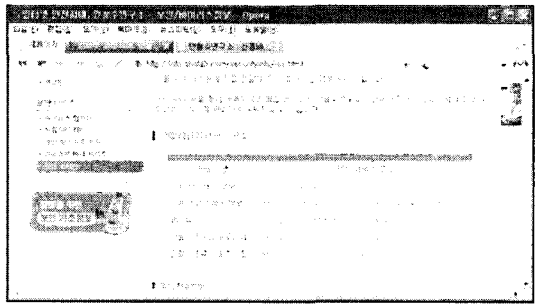
(그림 5) 테이블 단위로 수집

• 이미지형태의 웹사이트

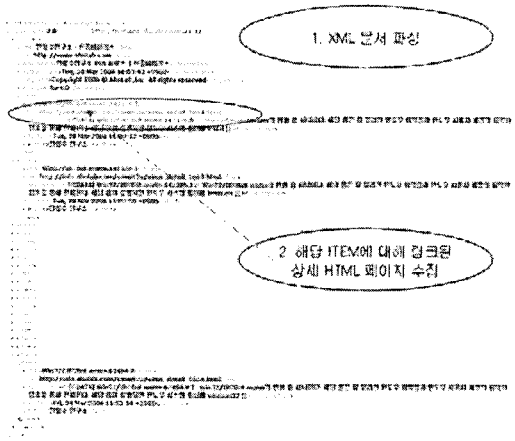
www.semantec.co.kr이나 www.krcert.or.kr과 같은 사이트들에서 제공하는 경보등급 정보는 대부분 이미지 형태를 취하고 있다. 이러한 이미지 형태의 웹사이트는 수집할 때 각 이미지를 해당하는 값에 매핑을 시켜 수집한다.

• RSS 지원 웹사이트

안철수연구소나, www.securityfocus.com, www.packetstromsecurity.nl과 같이 RSS 형태로 보안 취약점, 뉴스, Exploit 코드를 제공하는 사이트들에 대해서는 XML 형식의 RSS문서를 파싱한 후 최근에 저장되지 않은 item에 대해 해당 링크의 웹 페이지를 수집한다.



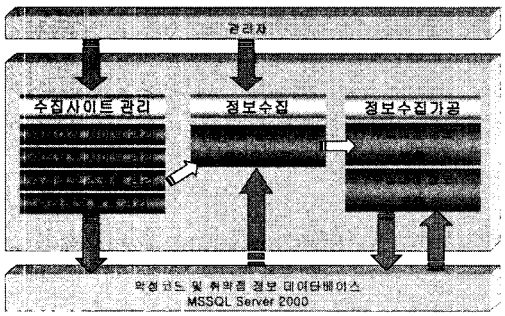
(그림 6) RSS 지원 웹사이트



(그림 7) XML 문서 파싱

WebCruiser의 기능은 아래와 같으며 전체 구성도는 (그림 8)에서 보는 바와 같다.

- 수집대상 사이트 관리 기능
  - 수집사이트 등록/조회/수정기능
- 수집정보 관리 기능
  - 수집정보 등록/조회/수정 기능
- 수집 스케줄 관리 기능
- 수집 스케줄에 따라 정보 수집 및 저장

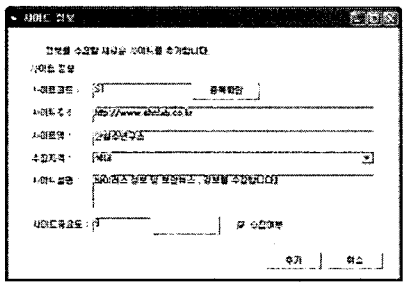


(그림 8) WebCruiser 구성도

WebCruiser의 동작 순서는 다음과 같다.

- 수집 사이트 등록

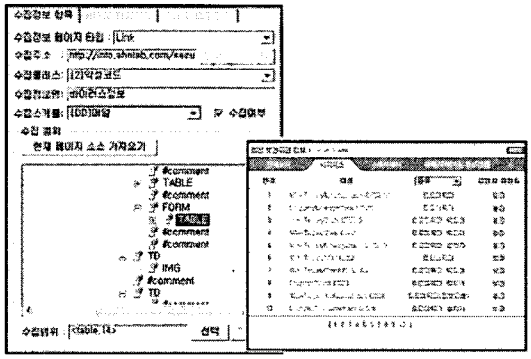
수집하려는 사이트 주소를 등록한다.



(그림 9) 수집 사이트 등록

- 수집항목 등록

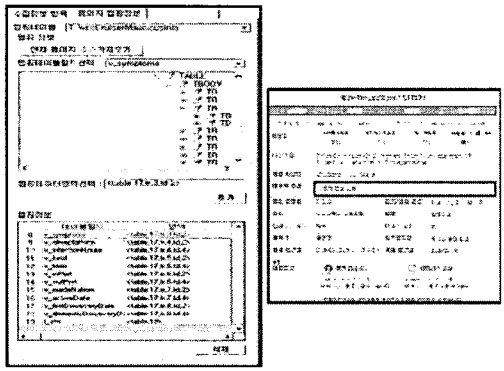
등록된 사이트로부터 웹 사이트의 구조를 분석하여 필요한 수집항목을 선택한다. 수집 항목을 등록 시 수집 클래스와 수집 스케줄을 함께 설정한다.



(그림 10) 수집항목 등록

- 페이지 맵핑

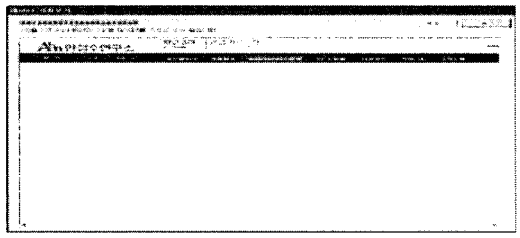
수집사이트의 수집항목 정보를 저장할 데이터베이스의 각 필드에 대한 맵핑 정보를 입력한다.



(그림 11) 수집항목의 저장 필드 맵핑

- 데이터 수집

해당 스케줄에 따라 데이터를 수집한다.



(그림 12) 데이터 수집 화면

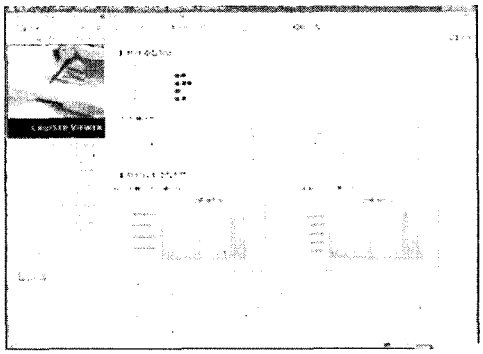
4.3 CruiserViewer 제작

CruiserViewer는 NetCruiser와 WebCruiser에서 보내온 정보를 전달 받아 데이터베이스에 저장하고 이를 웹을 통하여 사용자에게 보여준다.

CruiserViewer는 다음과 같은 기능을 수행한다.

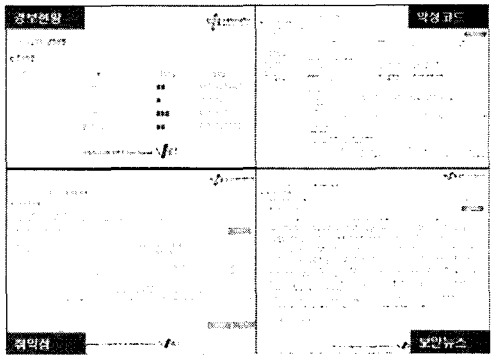
- WebCruiser 수집 정보 표시기
  - 수집 사이트의 검색/통계정보 표시
  - 수집 항목별 통계 정보 표시
  - 수집된 경보현황 정보 표시
  - 수집된 악성코드 정보 표시
  - 수집된 취약점 정보 표시
  - 수집된 보안뉴스 정보 표시
- NetCruiser 수집 정보 표시기
  - 수집 에이전트 이력 표시
  - 수집 항목별 통계 정보 표시
  - 네트워크 통계 정보 표시
  - 네트워크 flow 정보 표시
  - 탐지 이벤트 정보 표시

(그림 13)은 CruiserViewer 메인화면 구성이다. 메인화면은 WebCruiser와 NetCruiser로부터 수집된 정보들을 요약하여 보여주고 있다.

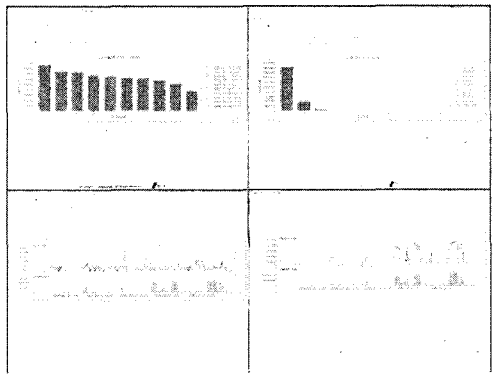


(그림 13) CruiserViewer 메인화면

(그림 14)는 WebCruiser로부터 수집된 정보들을 보여주는 화면이고 (그림 15)는 NetCruiser로부터 수집된 정보들을 보여주는 화면이다.



(그림 14) WebCruiser의 수집정보



(그림 15) NetCruiser의 수집정보

5. 결 론

본 논문은 사이버위협 관리를 위한 정보수집의 일환으로 네트워크 트래픽으로부터는 탐지이벤트와 각종 트래픽 통계 정보, 트래픽 특성분석에 많이 이용되는 flow정보와 같은 정량적인 정보를 수집하고 인터넷 웹 사이트로 부터는 취약점 정보, 웜·바이러스 같은 악성코드 정보, 경보발령 정보, 보안 뉴스 등의 정성적인 정보를 자동으로 수집하는 인터넷 위협 및 취약점 자동 수집기를 구현하였다.

제안된 수집기는 사이버위협을 관리하는데 있어 정량적인 정보 뿐 아니라 정성적인 정보를 함

께 수집함으로써 사이버위협 판단의 정확성을 높이고 아직 발생하지 않은 사이버 위협에 대응하기 위한 정보로 이용될 수 있다.

향후 연구되어야 할 내용은 네트워크의 발전에 따른 NetCruiser의 성능향상과 함께 정량적인 수집 항목에 대한 연구와 다양한 웹 사이트들의 구조를 분석할 수 있는 분석 기법에 대한 연구가 함께 이우러져야 하겠다.

참 고 문 헌

[1] 권기훈, 한영구, 정석봉, 김세현, 이수형, 나중찬, "트래픽 분석에 의한 광대역 네트워크 조기 경보 기법", 정보보호학회, 제14권 제4호, pp. 111-121, 2004. 8.

[2] A. Lakhina, M. Crovella, and C. Diot, "Characterization of Network-Wide Anomalies in Traffic Flows", Internet measurement Conference, 2004.

[3] A. Lakhina, M. Crovella, and C. Diot, "Mining Anomalies using Traffic Feature Distributions", BUCS-TR-2005-02, Technical Paper, Boston Univ., 2005.

[4] Myung-Sup Kim, Hun-Jeong Kang, and Seong-Cheol Hong, "A Flow-based Method for Abnormal Network Traffic Detection", IEEE /IFIP Network Operations and Management Symposium, Apr. 2004.

[5] Hyunsang Choi and Heejo Lee, "PCAV : Internet Attack Visualization on Parallel Coordinates", ICICS 2005, Beijing, China, December 10-13, 2005.

[6] 이민형, 이경호, "Multimedia Document Processing : Extracting Logical Structure from Web Documents", 한국멀티미디어학회, 2004.

[7] www.symantec.co.kr DeepSight

[8] www.ahnlab.com

[9] www.hauri.co.kr

[10] www.seurityfocus.com

이 은 영

2001년 아주대학교 정보및컴퓨터공학부(공학사)
2003년 한국과학기술원 전산학과(이학석사)
2003년~현재 국가보안기술연구소 연구원

백 승 현

1998년 한동대학교 전산전자공학부(공학사)
2001년 한국과학기술원 전산학과(이학석사)
2001년~2003년 ㈜아이디스 전임연구원
2003년~현재 국가보안기술연구소 연구원

박 인 성

2001년 동국대학교 정보산업과(경영학사)
2005년 경북대학교 컴퓨터과학과(이학석사)
2003년~현재 국가보안기술연구소 연구원

윤 주 범

1999년 고려대학교 컴퓨터학과(이학사)
2001년 서울대학교 컴퓨터공학과(공학석사)
2001년~현재 국가보안기술연구소 연구원

오 형 근

2000년 순천향대학교 전산학과(공학사)
2000년 KCP 기술개발부 선임연구원
2000년 8월~현재 국가보안기술연구소 선임연구원
2003년 9월~현재 고려대학교 정보보호대학원 박사과정 재학중

이 도 훈

1989년 한양대학교 전산학과(공학사)
1991년 한양대학교 전산학과(공학석사)
1991년~2000년 국방과학연구소 선임연구원
2000년~현재 국가보안기술연구소 선임연구원