상황 인식 모듈에 기반한 개인정보 통합 에이전트의 설계

김대유*, 김정태
(주)위너다임, 목원대학교

Design of Agent Integration for User Information Privacy Based on Situation Recognition Module

Dae-Yu Kim*, Jung-Tae Kim
Winnerdigm*, Mokwon University
E-mail : jtkim5068@gmail.com

요 약

본 논문에서 제시하는 통합 관리 지능형 에이전트 기술은 개인정보보호 사고의 원인분석을 통해 도출된 요구기능을 통합 구현하는 기술이다. 본 기술은 PC 및 인터넷 이용자들의 개인정보 침해에 따른 경제적 피해를 줄이고, 안전한 인터넷 문화를 정착하여 인터넷 이용자들의 인터넷 경제활동 활성화에 기여할 뿐만 아니라, 개인정보 노출방지 등을 통해 명의도용 등의 사고를 예방하여 실물경제활동도 촉진하는 효과가 있다. 먼저, 피싱·파밍 등의 개인정보 침해에 대응한 상황인식 기반 피싱·파밍 자동분석 기술을 적용함으로써 인터넷 사이트를 통한 경제활동의 신뢰가 확보되어 인터넷 금융, 온라인 쇼핑몰 등의 인터넷 경제활동을 촉진하게 되며, 개인정보 노출에 따른 피해를 줄임으로써 다양한 형태의 명의도용 사고를 방지할 수 있다.

Ⅰ. 서론

홈페이지를 통한 개인정보 노출이나 개인정보 보유자의 부주의로 인한 개인정보 유출 사고는 개인정보 보유자가 저장하고 있는 파일에 포함된 개인정보를 통해 발생하고 있으나, 현재는 웹기반 개인정보 필터링 기술만이 개발되어 있을 뿐, 시스템 내부의 파일을 점검하는 시스템기반 개인정보 필터링 기술은 아직 개발되지 않아서, 보유자는 PC 내에 저장하고 있는 파일 중 개인정보가 포함된 파일에 대해서는 관리를 하지 못하고 있다. 뿐만 아니라, 피싱, 파밍이 금년 초에 문제점으로 부각되면서 이러한 침해에 대응하기 위해 제안된 솔루션은 모두 블랙리스트 또는 화이트리스트 관리를 통한 점검 방식이어서 진화하는 다양한 침해기술에 대응하기에는 부적합하다. 더구나 PC 및 인터넷 이용자의 개인정보 문제는 PC 내부에 저장된 파일을 통한 노출 및 유출, PC 이용 시 접근한 피싱, 파밍 등 불법 사이트를 통한 유출 등으로 집약할 수 있는데, 이러한 기능들은 하나의 도구로 통합 관리할 필요가 있다. 따라서 PC 및 인터넷 이용자의 개인정보를 보호함으로써 경제적·정신적 피해를 예방하기 위해서는 피해사고의 원인에 대한 지능적인 대책기능을 제공하고 각 기능이 일관성 있게 통합 운영되는 “개인정보보호 통합 에이전트” 개발이 무엇보다도 중요하다.

II. 통합 에이전트의 블록 구성도

본 논문에서 개발하는 하고자하는 상황인식기반 개인정보보호 통합에이전트는 통합에이전트와 업데이트 서버로 구성되며, 통합에이전트의 모듈 구조를 나타내면 (그림 1)과 같다. 앞에서 설명한 상황인식기반 개인정보보호 통합에이전트의 모듈 세부 구조를 타나내면 다음 (그림 2)와 같다.

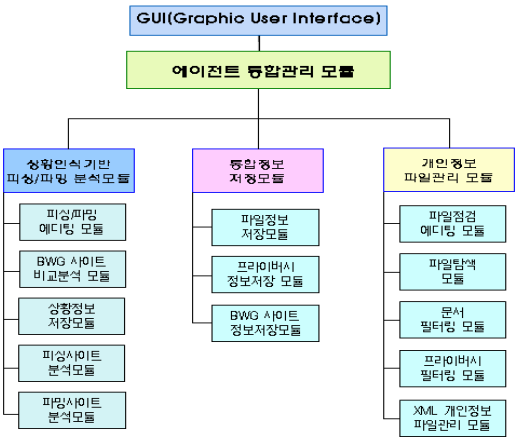

그림 1. 에이전트별 기능 분류

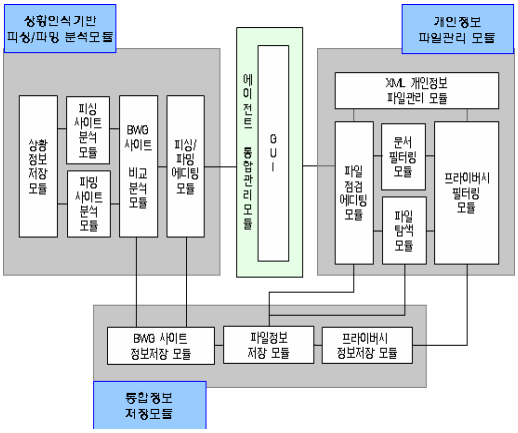

그림 2. 모듈별 세부 구조

III. 개발 환경

가. 프로그램 사용 환경

항목	최소사양	권장사양
CPU	Intel Pentium 150MHz	Intel Pentium Ⅱ 400MHz
RAM	32MB	128MB
HDD	10MB	20MB
VGA	800x600 256Color	1024x768 16bit or 32bit
OS	Microsoft Windows 98/Me/NT/2000/XP (x86, x64)	
Web Browser	Microsoft Internet Explorer 4.0, 5.0, 6.0, 7.0	

나. 시스템 구성도

통합에이전트 시스템의 처리 과정은 3단계로 이루어져있다. 사용자가 사용하려는 프로세스를 검사하는 통합에이전트가 있으며, 각 피싱/파밍/개인정보관리 에이전트는 브라우저나 시스템의 호스트 또한 개인정보를 관리한다. 웹 브라우저, 시스템의 호스트, PC의 문서는 3개의 에이전트를 통하여 감시하여 보호 할 수 있다.

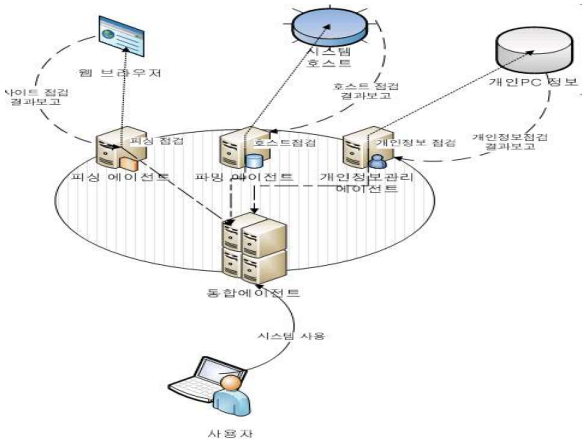

그림 3. 시스템 전체 구성도

가. 상위 모듈

통합에이전트 화면의 각 에이전트를 실행 및 설정할 수 있는 GUI 이며, 각 에이전트의 화면 구성(사이트 관리, 호스트 관리, 디렉토리 점검, 자동 업데이트)로 구성 되어 있으며, 각 화면의 설명은 은 다음 표와 같다

<표 1> 통합에이전트 메인 모듈 설명

메뉴구성	설 명
사이트 관리	피싱 및 파밍 사이트로 접근하는 것을 설정하는 GUI
호스트 관리	사용하려는 PC의 도메인 호스트 정보를 검사하는 GUI
디렉토리 점검	사용하려는 PC의 특정 디렉토리의 개인정보를 점검 및 결과 보고하는 GUI
자동 업데이트	각 에이전트의 버전을 검사하여 자동 업그레이드 하는 GUI

나. 에이전트 통합 관리 모듈

Tray 창의 기본 에이전트 기능으로 웹사이트 접속 이벤트를 확인하여 해당 하위 모듈에 전달하는 기능과 GUI를 통해 받은 실행명령을 하부 모듈에 전달하는 제어 기능 및 업데이트를 포함한 하위 모듈간의 실행 관리 등의 전체적인 관리기능을 수행한다.

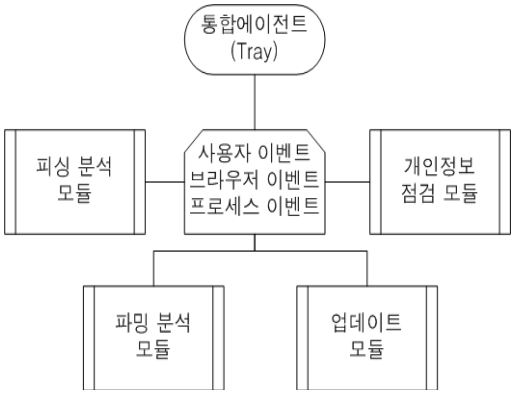

그림 4. 관리모듈의 기능도별 연관도

IV. 실험 및 고찰

현재 운영되고 있는 웹 사이트의 목록을 임의로 (B/W/G)사이트로 등록하여, 상황인식기반 피싱/파밍 에이전트의 실험데이터로 사용하였다. 안전사이트 항목은 인터넷 포털(랭키닷컴)에서 제공하는 2008년 8월 사이트 순위 200위중 1~25까지의 항목을 실험데이터로 사용하였다. 차단사이트 항목은 인터넷(urlblacklist.com)에서 제공하는 2008년 7월 유해 사이트 항목 3천 건의 데이터 중 25가지의 항목을 전제로 실험데이터로 사용하였다.

IV. 결론

본 논문을 통해 제안한 “상황인식 기반의 통합 개인정보보호 에이전트 시스템”을 개발하였다. 개발된 시스템은 크게 피싱/파밍에이전트, 디렉토리 개인정보보호 에이전트로 구성되어 있다. 개발된 “상황인식 기반의 통합 개인정보보호 에이전트 시스템”은 BHO(Browser Helper Object) 기술을 사용하였다. 개발된 “상황인식 기반의 통합 개인정보보호 에이전트 시스템”은 BHO(Browser Helper Object) 기술을 사용하였다. 대부분의 이용자들이 Windows운영체제에서 제공하는 Internet Explrer Browser를 사용하기 때문이다. 이 BHO 기술은 브라우저의 이벤트 핸들링 메시지를 제어 할 수 있기 때문에, 인터넷으로 피싱/파밍사이트로 접근할 때, 이동되는 주소를 BWG 항목과 비교 분석하여 “상황인식 기반 통합개인정보보호 에이전트 시스템”의 사용자는 “피싱/파밍”사이트로부터 보호 받을 수 있다.

참고문헌

[1] Anti-Phishing Working Group, http://www.antiphishing.org, 2005.

[2] W. Liu, X. Deng, G. Huang, and A.Y. Fu, “An Anti-Phishing Strategy Based on Visual Similarity Assessment,” IEEE Internet Computing, vol. 10, no. 2, pp. 58-65, 2006.

[3] D. Martin, H. Wu, and A. Alsaid, “Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use,” Communication of the ACM, vol. 46, no. 12, 2003, pp. 258 264.

[감사의 글]

본 논문은 2010년도 한국과학기술단체총연합회의 지원을 받아 “이공계전문가기술지원서포터즈 기업 및 맞춤형멘토지원사업”에서 수행된 기초연구사업입니다.