사용자 행위 추적 시스템의 그래프 분석 도구 개발에 관한 연구

이윤경, 정수정, 송수경, 이민수
이화여자대학교 컴퓨터정보통신학과
e-mail: narouge@ewhain.net

A Study on Development of a Graphical Analysis Tool for the User Behavior Tracing System

Yoon-Kyung Lee, Su-Jeong Cheong, Soo-Kyung Song, Min-Soo Lee
Dept of Computer Science, Ewha Womans University

요 약

사용자의 행동 모니터링에 대한 이전의 기술적인 연구는 네트워크 트래픽과 데이터베이스 접근 형태에 집중되어 왔다. 이전의 연구는 자료를 공유하고 교환하는 것 같은 사용자들 사이의 상호작용을 관찰하는 부분에 있어서는 부족하다. 즉, 사용자와 사용자의 행동 정보를 수집하고 그 자료에 바탕을 두고 상호작용을 시각적으로 관찰할 수 있어야 한다. 따라서 수집된 자료의 좀 더 분석적인 관찰을 위해서 지금까지의 개발되고 사용된 여러 가지 컴포넌트를 사용하여 이 같은 상호작용을 여러 가지 형태의 그래프로 표현할 수 있는 그래픽 툴을 개발한다.

1. 서론

사용자의 행동 모니터링에 대한 이전의 기술적인 연구는 네트워크 트래픽과 데이터베이스 접근 양식에 집중되어 왔다. 이런 접근법들은 공동 연구 환경에서 자료를 공유하고 교환하는 사용자들 간의 상호작용을 관찰하는 부분에 있어서는 부족한 점이 있다. 공동 네트워크처럼 주어진 어떤 주제에서 관련된 문서에 나타난 사용자의 행위에 대한 모니터링은 적절한 행동이 될지도 모르는 행위를 자동적으로 막지 않고 사용자와 행위들을 공격하는 것을 식별하는 것을 최대한 돕는다.

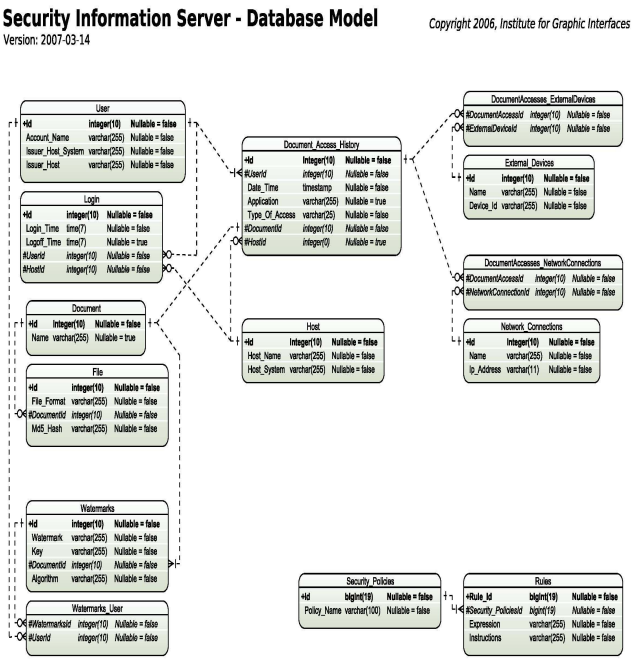
이러한 행위들은 사용자의 행동들을 효과적으로 분석하고 감시하기 위한 사용자들에게 도움을 주기 위해 그래픽한 형태로 보여줄 수 있었다. 따라서 이 시스템은 사용자의 행동을 모니터링하는 시스템과 같은 그래픽 분석 도구를 개발하는 데에 그 목표를 두고 있다.

2. 그래프를 통한 사용자의 행위 패턴 분석

가상 엔지니어 환경을 위한 사용자 행동 추적 시스템은 문서상으로 사용자의 행동들을 모니터링하기 위한 기능성을 제공한다. 이 시스템에 의해 습득된 정보는 중앙 서버, 즉 보안 정보 서버에 저장되고 다음과 같이 분류 된다.

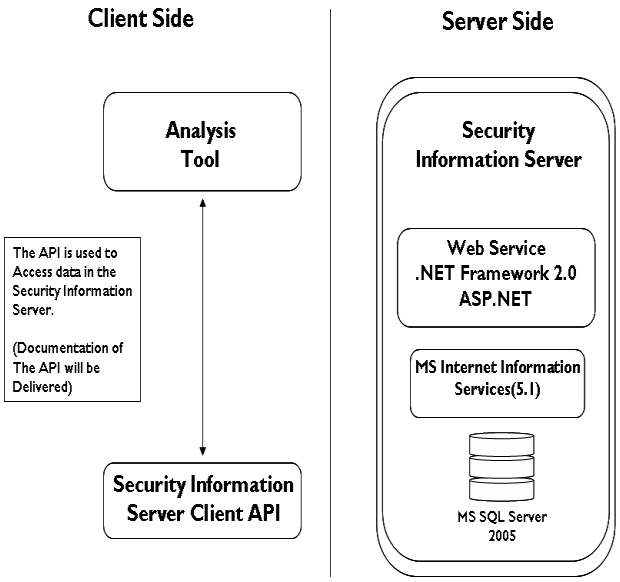
접근된 문서에 대한 정보에는 접근 날짜 및 시간, 접근 유형(읽기/쓰기), 사용된 응용 프로그램, 사용자 신분, 어떤 문서에 접근했는지 등의 정보가 들어있다.

문서 접근이 발생한 환경에 대한 정보에는 호스트 네임(컴퓨터 이름). 워크스테이션과 연결된 외부 장치들, 워크스테이션에 대한 활성화된 네트워크 연결 등의 정보가 들어있다. 이 시스템은 사용자 행동을 감지할 수 있을 것이다.



<그림1. database model>

이 시스템의 첫 번째 작업은 수집된 사용자 행동 정보를 그래프로 보여주기 위해 사용될 소프트웨어 툴을 개발하는 것이다. 그 툴은 사용자 행동에 대한 자료는 좀 더 효율적인 분석을 지원하기 위해 사용자가 많은 그래프의 표현 방식들 중에서 선택할 수 있도록 개발될 것이다. 2D, 3D, scatter, bubble 형태 등의 여러 가지 그래프 형태들로 자료를 표현하여 화면에 정밀하게 표시되어 질 수 있다.



<그림1. 클라이언트와 서버 관계도>

클라이언트는 서버의 Security Information Server의 Client API를 이용하여 DB에서 원하는 자료를 가져다가 그래픽 툴을 이용하여 자료에 대한 분석을 하여 원하는 수가 있다.

3. 결론

미래에 이 소프트웨어 툴은 사용자 행동 정보, 정의 그리고 사용자 행동 방식의 관리의 시각화를 위한 더 큰 응용 프로그램의 일부분이 될 것이다. 응용 프로그램에 대한 소프트웨어 툴이 기여하는 부분은 시각화와 그래프의 일정부분에 대한 페인팅 컴포넌트를 추가할 수 있도록 하는 API이다. 소프트웨어는 또한 페인팅 컴포넌트를 가진 더 많은 확장성을 갖는 API를 제공해야만 한다.

많은 테스트와 데모를 통해서 가능한 시뮬레이트된 사용자 행동 정보를 가진 보안 정보 서버의 데이터베이스를 가진 소프트웨어 또는 SQL의 개발이 필요하다.

* 본 연구는 IGI의 지원을 받아 수행되었습니다.

참고문헌

[1] Juval Lowy, "COM and .NET Component Services", O'Reilly, 2001

[2] Faison, Edmund W. J., "Component-Based Development With Visual C#", John Wiley & Sons Inc, 2002

[3] Joe Duffy "Professional .NET Framework 2.0", Wrox, 2006

[4] Lowy, Juval, "Programming.NET Components", Oreilly & Associates Inc ,2005

[5] Bill Evjen, Scott Hanselman, Farhan Muhammad, Srinivasa Sivakumar, Devin Rader, "PROFESSIONAL ASP.NET" Wrox, 2006

[6] Lee, Wei Meng, Jepson, Brian , "Programming the .Net Compact Framework", Oreilly & Associates Inc, 2006

[7] Chappell, David ," Understanding .NET 2/e" , Addison-Wesley , 2006.