# 웹 클라이언트 연결 정보 모니터링 설계 및 구현

조아라*, 정치윤**, 장범환**, 나중찬**
*과학기술연합대학원 정보보호학과
**한국전자통신연구원 지식정보보안연구부 보안관제기술연구팀
e-mail:{joara11, iamready, bchang, njc}@etri.re.kr

# Monitoring Environment Design for Web Connection Information

A-Ra Jo*, Chi-Yoon Jeong**, Beom-Hwan Chang**, Jung-Chan Na**
*Division of Information Security, University of Science and Technology.
**Managed Security Research Team, Knowledge-based Information Security & Safety Research Division, ETRI.

요 약

최근 웹 서비스 환경에서 공격자가 자신의 근원지를 은닉하기 위하여 여러 단계의 경유지를 거쳐 공격을 시도하는 사례가 증가하고 있으며, 이에 대한 법률적 증거 확보 및 능동적인 대처를 위하여 웹 어플리케이션에서의 역추적 기술이 필요하다. 현재 자바 애플릿이나 ActiveX, 플러그인, 웹 로그 등을 이용한 응용 계층의 추적 기술이 개발되고 있지만, 웹 클라이언트에 의하여 차단될 가능성이 높고, 플러그인 종류 및 호환되지 않는 운영 환경 등 제약조건으로 인하여 사용에 제한이 있다. 본 논문에서는 액션 스크립트를 이용한 웹 클라이언트 모니터링 시스템을 제안한다. 제안된 시스템은 웹 클라이언트가 실행을 인식하지 못하고 수행되어 웹 클라이언트에 의한 차단을 막을 수 있고, 다양한 운영 환경에서 사용이 가능하다.

## Ⅰ. 서 론

네트워크 인프라의 발전으로 인하여 인터넷이 급격하게 확산되면서 인터넷의 영향력은 사회 전반에 점차 확대되고 있다. 이에 대한 역기능으로 분산서비스거부(DDoS) 공격, 해킹 등 사이버 공격의 발생 빈도가 높아지고 있으며, 그 피해 규모도 점점 방대해지고 있다. 사이버 공격으로 인한 피해가 국가 차원의 문제로 부각되고 있음에도 불구하고, 대응책의 미흡함으로 인하여 경제적 피해 및 사회적 손실이 여전히 증가하고 있는 실정이다.

특히 인터넷 뱅킹을 통한 금융 사고가 증가하면서 전자상거래 보안의 중요성이 강조되고 있다. 2007년 개정된 전자금융거래법에 따르면, 금융기관 및 전자금융거래기관은 보안사고 발생 시 책임 소재를 입증할 수 있는 법률적 증거를 확보해야한다고 명시하고 있다. 만약 금융기관이 법률적 증거를 확보하지 못할 경우, 해당 기관이 사고에 대한 책임을 져야한다. 따라서 금융기관은 사용자의 접속 시간, 접속 근원지 등의 연결 정보를 확보해야한다. 금융기관뿐 아니라 각 정부부처 및 웹 사이트 운영자들도 보안사고 발생 시 책임 소재를 입증할 자료를 필요로 한다.

사이버 공격에 대한 대응 및 증거 확보를 위하여 공격의 근원지를 찾는 역추적 기술이 개발되고 있으며, 현재 주로 개발되는 기술은 IP 계층 기반의 역추적 기술이다. IP 계층 기반의 역추적 기술은 네트워크 과부하, 패킷 위조의 위험 등의 이유로 웹 환경에 적용이 힘들다. 따라서 웹에서 이용 가능하도록 자바 애플릿, 플러그인 등을 이용한 응용 계층 기반의 역추적 기술이 개발되고 있다. 하지만 기존 응용 계층 기반의 역추적 기술은 공격자에 의하여 수행이 차단될 수 있으며, 추적에 사용되는 플러그인 종류의 제약 등의 문제점이 있다. 따라서 본 논문에서는 상기 문제점을 해결하기 위하여 액션 스크립트를 이용한 웹 클라이언트 연결 정보 모니터링 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 IP 계층 기반의 역추적 기술과 응용 계층 기반의 역추적 기술에 대하여 살펴보고, 3장에서는 본 논문에서 제안한 액션 스크립트를 이용한 웹 서버 모니터링 기술에 대해서 설명할 것이다. 4장에서는 본 기술의 효과와 향후 연구 방향 등에 관하여 이야기하며 결론을 내릴 것이다.

## Ⅱ. 관련 연구

### 1. IP 계층 기반의 역추적

#### 1.1. TCP 역추적 기법

TCP 역추적 기법은 호스트 기반과 네트워크 기반의

본 연구는 지식경제부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S-022-03, All-IP 환경의 지능형 사이버공격 감시 및 추적 시스템]

역추적 기법으로 나눌 수 있다. 호스트 기반의 역추적 기법은 호스트에서의 로그 기록을 이용하여 공격 근원지를 추적하는 방법으로, 공격선상의 모든 호스트에 역추적 모듈을 설치해야 한다는 단점이 있다.[1] 네트워크 기반의 역추적 기법은 네트워크에서 송수신되는 패킷으로부터 공격에 사용된 연결 경로 정보를 추출하고 해당 연결에 대한 정보를 이용하여 역추적을 수행하는 기법이다.[2] 연결 정보를 수집하기 위해서 라우터에 패킷을 모니터링 할 수 있는 역추적 모듈을 설치해야 된다는 취약점을 지닌다.

TCP 역추적 기법의 두 방법은 역추적을 수행하려는 모든 곳에 역추적 모듈을 설치해야하기 때문에 실제 환경에서는 적용이 불가능하다.

### 1.2. IP 역추적 기법

IP 역추적 기법에는 로깅, 링크 검사, 오버레이 네트워크 기반, 확률적 패킷 마킹, ICMP 기반, IPSec 기반의 역추적 기법이 있다.

로깅 기법은 라우터를 통과하는 패킷을 저장하여 공격 경로를 추적하는 방법으로 라우터를 통과하는 모든 패킷을 저장하기 때문에 많은 저장 공간이 필요하지만, 이 정보를 사용하여 사후 추적이 가능하다는 장점도 있다.[3]

링크 검사법은 피해 호스트에 근접한 라우터를 시작으로 공격 트래픽이 유입된 라우터를 순차적으로 검사하는 hop-to-hop 추적 방법이다.[4] 링크 검사법은 패킷의 전송 경로를 조합, 판별할 수 있지만, 공격이 끝난 후에는 추적 할 수 없다는 단점이 있다.

오버레이 네트워크 기반의 역추적 기법은 호스트에 연결된 라우터에서 전달된 정보를 네트워크 안에 도입된 추적용 라우터를 통하여 감시하는 기법이다.[5] 추적용 라우터에서 수집된 정보를 재구성하여 패킷의 경로를 분석하여 공격의 근원지를 추적한다.

확률적 패킷 마킹 기법은 IP 헤더 중 변형 가능한 필드에 라우터의 주소 정보를 마킹하여 다음 라우터로 전달한 후, 공격 발생 시 피해 호스트에 수신된 패킷의 정보를 이용하여 공격 경로를 재구성하는 방법이다.[6]

ICMP 기반의 역추적 기법은 샘플링한 패킷에 대하여 이전 단계 라우터의 정보와 다음 단계 라우터 정보, 패킷의 페이로드 등을 포함한 ICMP 역추적 메시지를 생성하고 목적지로 전송하여 목적지에서 공격 경로를 판별하는 방법이다. ICMP 기반의 역추적 기법은 공격 중에는 물론, 공격이 종료된 후에도 추적이 가능하다.[7]

IPSec 기반의 역추적 기법은 네트워크상의 라우터와 피해 시스템 간에 IPSec 연결 한 후, 공격 패킷이 해당 라우터를 통해 전송될 경우 IPSec 터널을 통하여 경로 정보를 피해 시스템에 전달하는 방법이다.[8]

지금까지 살펴본 IP 역추적 기법의 특징들을 비교하면 [표 1]과 같다. [표 1]을 보면, 로깅 기법, 확률적 패킷 마킹 기법, ICMP 및 IPSec 기반의 역추적 기법은 메모리

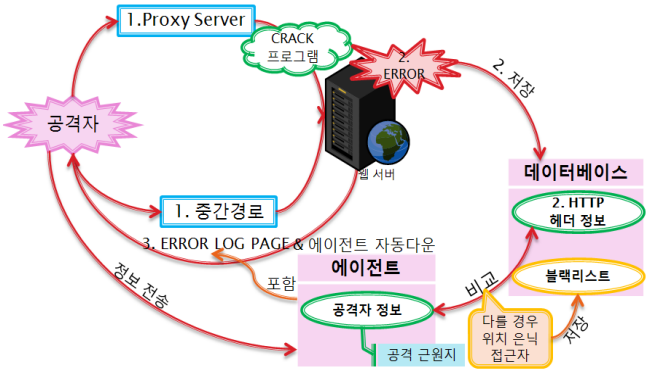
〔표 1〕 IP 역추적 기법의 특징 비교

| 구분 | 기법 / 특성 | 로깅 | 링크 검사 | 오버레이 | 확률적 패킷마킹 | ICMP 기반 | IPSec |
|---|---|---|---|---|---|---|---|
| 오버헤드 | 네트워크 부하 | N/A | Low | High | Low | Low | High |
| | 피해시스템부하 | N/A | N/A | N/A | High | High | High |
| | 라우터 부하 | High | High | Low | Low | Low | High |
| 요구사항 | 라우터 변경 | No | No | No | Yes | Yes | No |
| | 에이전트 여부 | Yes | No | No | No | No | Yes |
| | 메모리 요구량 | High | Low | Low | High | High | Low |
| 성능 | 신속성 | Moderate | Moderate | Good | Bad | Bad | Moderate |
| 공격대응 | DDoS 대응 | Bad | Good | Good | Bad | Bad | Bad |

요구량이 높아 DDoS 공격 등과 같은 방대한 양의 트래픽을 생성하는 공격에 취약하다. 이 기술들은 많은 접속자들로 인하여 DDoS 공격과 유사한 트래픽이 생성되는 웹 어플리케이션에 적용하기에는 어려움이 있다. 또한 DDoS 공격에 대한 대응이 가능한 오버레이 네트워크 기반의 역추적 기법의 경우, 네트워크 부하의 위험성이 높아 웹 어플리케이션에 적용이 어렵다. 링크 검사법의 경우 관리 도메인 이외의 라우터에 접속하는 것이 불가능하여 다수의 도메인으로부터 트래픽이 유입되는 웹 어플리케이션 환경에 적용할 수 없다. 따라서 웹 어플리케이션에서 적용 가능한 응용 계층 기반의 역추적 기술이 필요하다.

## 2. 응용 계층 기반의 역추적

### 2.1. 자바 애플릿을 이용한 웹 클라이언트 모니터링 기술

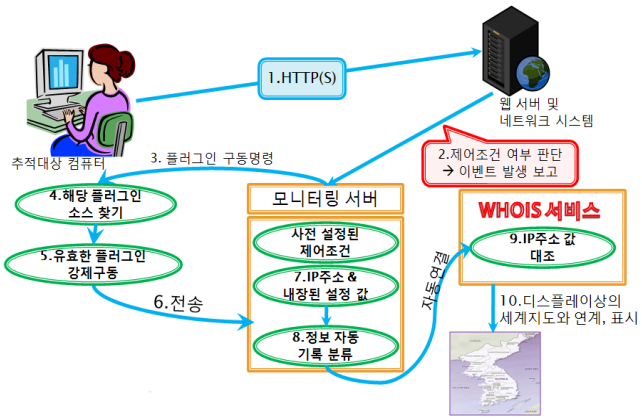



[그림 1] 자바 애플릿을 이용한 공격자 추적 시스템의 흐름도

자바 애플릿을 이용한 공격자 추적 방법은 공격자로 하여금 에이전트 기능을 하는 자바 애플릿을 다운 받도록 하여 에이전트에서 수집한 정보를 사용하여 공격의 근원지를 찾는 방법이다. 자바 애플릿을 이용한 공격자 추적 방법의 흐름도는 [그림 1]과 같다. 웹 서버에서 추출한

HTTP 헤더의 정보로부터 공격자가 경유한 중간 경로를 알 수 있고, 에이전트가 수집한 정보로부터 공격자의 실제 위치를 파악할 수 있다. 두 정보의 위치가 다를 경우에는 위치 은닉 접근자로 분류하여 블랙리스트로 저장한다.[9]

### 2.2. 플러그인을 이용한 웹 클라이언트 모니터링 기술




[그림 2] 플러그인을 이용한 웹 클라이언트 모니터링 기술의 흐름도

플러그인을 이용한 웹 클라이언트 모니터링 기술은 공격자가 웹 서버에 접속할 때 모니터링 서버에서 공격자의 PC에 설치된 플러그인을 강제로 구동시켜 공격자 위치를 추적하는 기술로써, 그에 따른 추적 방법은 [그림 2]와 같다. 공격자의 PC에 설치된 강제 구동에 사용되는 플러그인은 웹 브라우저에 내재되는 플러그인 형태이며, 양방향 및 소켓통신을 지원해야 한다. 플러그인을 이용한 방법의 경우 상기 조건을 만족할 시에만 정상적으로 동작하여 접속자의 근원지 및 접속자의 PC에 내장된 각종 설정 값, 중간 경유지 등의 정보를 추출할 수 있다.[10]

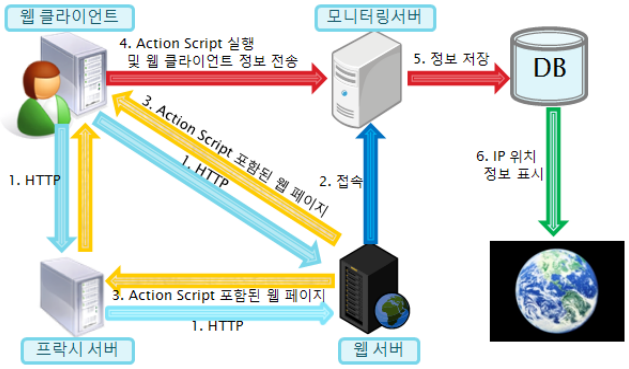
### 2.3. 웹 로그를 이용한 웹 클라이언트 모니터링 기술

웹 로그를 이용한 웹 클라이언트 모니터링 기술은 네트워크에서 전송되는 패킷 중 웹 서비스와 관련된 패킷만을 수집하여 실시간으로 저장하고 감시하는 기술이다. 수집된 패킷 중 사전 정의된 유해 IP의 로그만을 실시간으로 필터링하여 저장, 분석할 수 있다.[11]

응용 계층 기반의 역추적 기술은 공격자에 의해 기능 수행이 차단 될 수 있고, 플러그인 및 운영 환경 등의 제약 사항으로 인하여 사용상에 제한이 있다. 따라서 본 논문은 상기 제약조건을 해결하기 위하여 액션 스크립트를 이용한 웹 클라이언트 모니터링 시스템을 제안한다.

## III. 액션 스크립트를 이용한 웹 클라이언트 모니터링 시스템

본 논문에서는 액션 스크립트를 이용하여 웹 클라이언트의 연결 정보를 모니터링 할 수 있는 시스템을 제안한다. 액션 스크립트의 경우 플래시 플레이어에서 동작하기 때문에 운영체제의 제한을 받지 않으며, 플래시 플레이어는 전 세계 PC의 99% 이상 설치되어 있어 플러그인의 제약 조건으로부터 자유로울 수 있다.[12] 또한 제안된 방법은 웹 클라이언트가 액션 스크립트를 포함한 웹 페이지에 접속하면, 접속과 동시에 웹 클라이언트의 PC에서 액션 스크립트가 자동으로 실행되기 때문에 웹 클라이언트가 자신의 접속 정보가 서버로 전송되는 것을 인지할 수 없다는 장점이 있다.




[그림 3] 액션 스크립트를 이용한 웹 클라이언트 모니터링 시스템의 흐름도

본 논문에서 제안된 모니터링 시스템의 흐름도는 [그림 3]과 같다. 웹 클라이언트가 웹 서버에 접속하면, 웹 클라이언트는 웹 페이지와 함께 액션 스크립트를 다운 받게 되며, 이 때 액션 스크립트가 자동으로 실행된다. 웹 클라이언트의 PC에서 실행된 액션 스크립트는 웹 클라이언트의 정보를 모니터링 서버로 전송한다. 모니터링 서버는 해당 패킷을 분석하여 IP 정보와 함께 접속 근원지 IP 및 프락시 IP의 지리 정보를 데이터베이스에 저장한다.

모니터링 서버는 저장하는 정보는 [그림 4], [그림 5]와 같다. 모니터링 서버에서는 웹 클라이언트가 웹 서버에 접속 했을 때 추출된 접속 IP를 IP 필드에 저장하고, 액션 스크립트의 실행을 통하여 추출되는 접속 IP 정보는 AS Client 필드에 저장한다. 모니터링 서버에서는 저장된 두 IP 정보를 비교하여 중간 경유지 또는 프락시 서버의 사용 여부를 검사하며, [그림 4]와 같이 IP와 AS Client 필드의 IP 주소가 다른 경우 프락시 서버를 사용한 사용자로 분류된다. [그림 5]와 같이 IP와 AS Client 필드의 IP 주소가 같은 경우 프락시 서버를 사용하지 않는 사용자로 분류 되게 된다. 모니터링 서버에서는 데이터베이스에 접속자 및 중간 경유지의 IP 정보로부터 IP주소 매핑 라이브러리를 사용하여 추출한 각 IP별 지리 정보 및 ISP정보를 같이 저장하게 된다.

본 논문에서 기존 응용 계층 기반의 역추적 기술의 문제점을 해결하기 위해서 액션 스크립트를 사용하는 방법을 제안하였다. 본 논문에서 제안된 방법과 기존 방법들의 특성을 비교해보면 [표 2]와 같다. 제안된 방법은 기존의 자바 애플릿, ActiveX 기반의 방법들과 달리 각종 보안 설정에 의하여 차단되지 않고, 클라이언트가 인지하지 못하게 실행 될 수 있다. 또한 ActiveX 기반의 방법은 특정

```
AS Client       : 125.248.82.129

IP              : 213.41.71.164
Webserver       : 129.254.242.205
URL             : http://129.254.242.205/index.html

countryCode     : KR
countryName     : Korea, Republic of
latitude        : 37.566406
longitude       : 126.999695
ISP             : DACOM-PUBNETPLUS

countryCode     : FR
countryName     : France
latitude        : 48.899994
longitude       : 2.399994
ISP             : COLT Telecom GmbH
Connection released ......
```

〔그림 4〕 프락시 서버 사용 시 저장되는 데이터

```
AS Client       : 125.248.82.129

IP              : 125.248.82.129
Webserver       : 129.254.242.205
URL             : http://129.254.242.205/index.html

countryCode     : KR
countryName     : Korea, Republic of
latitude        : 37.566406
longitude       : 126.999695
ISP             : DACOM-PUBNETPLUS

countryCode     : NO PROXY
countryName     : NO PROXY
latitude        : NO PROXY
longitude       : NO PROXY
ISP             : NO PROXY
Connection released ......
```

〔그림 5〕 프락시 서버 미사용 시 저장되는 데이터

운영 체제에서만 실행이 가능하지만, 제안한 방법은 다양한 운영체제에서 실행 가능하다는 장점이 있다. 플러그인을 사용하는 방법의 경우 각종 제약 조건을 만족하는 웹 브라우저의 플러그인만을 사용할 수 있지만, 액션 스크립트는 제약조건이 적어 보다 유연하게 사용할 수 있다. 웹 로그 기반의 방법은 모든 웹 로그를 수집하여 저장하기 위하여 많은 메모리가 필요하지만, 제안한 시스템은 접속과 관련된 정보만을 추출하여 저장하기 때문에 메모리의 요구량이 적다는 장점이 있다.

〔표 2〕 제안한 시스템과 기존 기법과의 특성 비교

| 기법 / 특성 | 자바 애플릿 /ActiveX | 웹 브라우저 플러그인 | 실시간 로그 분석 | 액션 스크립트 |
|---|---|---|---|---|
| 에이전트 필요성 | Yes | Yes | No | Yes |
| 메모리 요구량 | Low | Low | High | Low |
| 정보의 다양화 | High | Low | Low | Low |
| 보안 설정에 의한 차단 | Yes | 조건 안 맞을 경우 Yes | N/A | No |

## Ⅳ. 결 론

본 논문에서는 웹 클라이언트의 연결 정보를 모니터링하기 위하여 액션 스크립트를 이용한 웹 클라이언트 모니터링 기술을 제안하였다. 액션 스크립트의 경우 플래시 플레이어에서 동작하기 때문에 운영체제의 제한을 받지 않으며, 제안된 방법의 경우 웹 클라이언트가 액션 스크립트를 포함한 웹 페이지에 접속하면 액션 스크립트가 자동으로 실행되기 때문에 웹 클라이언트가 자신의 접속 정보가 서버로 전송되는 것을 인지 할 수 없다는 장점이 있다. 또한 제안된 방법은 자신의 위치를 은닉하여 웹 서버에 접속하는 공격자의 근원지는 물론 은닉에 사용된 프락시 서버의 정보까지도 추출할 수 있다.

제안된 방법의 경우 자바 애플릿이나 ActiveX 기반의 방법에 비하여 클라이언트의 호스트에서 수집 할 수 있는 정보가 한정되어 있다는 문제점이 있다. 향후에는 액션 스크립트와 다른 기법의 혼용을 통하여 보다 많은 정보를 웹 클라이언트 모르게 추출 할 수 있는 방법에 대한 연구가 필요하다.

## 참고문헌


[1] H.T. Jung et al. “Caller Identification System in the Internet Environment,” The 4th Usenix Security Symposium, 1993.

[2] D. W. Song, A. Perrig, “Advanced and Authenticated marking Schemes for IP Traceback,” InfoCom 2001.

[3] C. Gong, K. Sarac, "IP traceback based on packet marking and logging," in IEEE International Conference on Communications (ICC), Seoul, Korea, 2005.

[4] H. Burch, B. Cheswick, “Tracing Anonymous Packets to Their Approximate Source,” Proc. USENIX LISA, 2000, pp. 319 - 27.

[5] R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," in Proc. 2000 USENIX Security Symp. 2000.7. pp. 199-212.

[6] S. Savage et al., “Network Support for IP Traceback,”IEEE/ACM Trans. Net., vol. 9, no. 3, June 2001, pp. 226 - 37.

[7] S. M. Bellovin, “ICMP Traceback Messages,” IETF draft, 2000.

[8] H.Y. Chang et al., “Deciduous: Decentralized Source Identification for Network-Based Intrusions,” Proc. 6th IFIP/IEEE Int’l. Symp. Integrated Net. Mgmt., 1999.

[9] 김태봉, 최운호, “역추적 기술의 동향 및 적용 사례 분석”, 정보보호학회지, 2005.2.

[10] 국경완, 이상훈, “TCP/IP 프로토콜 취약성 공격 탐지를 위한 실시간 접근 로그 설계 및 구현”, 한국정보과학회 학술발표논문집, 2001.

[11] 이인희, 박대우, “IP 역추적 설계 및 보안감사 자료생성에 관한 연구”, 한국컴퓨터정보학회 하계학술발표논문집 및 학회지, 2007.

[12] Millward Brown survey, "Flash Player Penetration", www.adobe.com/products/player_census/flashplayer/