프라이버시 보호형 환경 평가 핑거프린팅 프레임워크 제안

박소영, 손예진*, 정헌영**, 목정현***, 이석준****, 서정택*****

가천대학교

(so030604, yejin1590*, wgdweg608**, johnmok***, junny****, seojtgt*****)@gachon.ac.kr

Privacy-Preserving Fingerprinting Framework for Client Environment Assessment

SoYoung Park, Son Ye Jin*, Jung Hun Young**,Jung-Hyun Mok***,Sokjoon Lee****, Jung Taek Seo*****

Gachon Univ.

요 약

본 논문에서는 핑거프린팅 제공업체가 사용자의 실행 환경 세부 정보를 중앙 서버로 수집 및 관리함으로써 발생하는 프라이버시 문제를 해결하면서도, 사용자 식별, 봇 탐지, 취약한 실행 환경 관리 기능을 유지하기 위해 프라이버시 보호형 환경 평가 핑거프린팅 프레임워크를 제안한다. 제안한 프레임워크는 사용자의 실행 환경 세부정보의 외부 노출을 차단하고 도메인 단위 사용자 식별과 클라이언트 측 환경 평가를 결합한 구조를 제공한다. 또한 구현 및 실험을 통해 제안한 프레임워크가 프라이버시 보호와 기존의 핑거프린팅 기능을 동시에 만족함을 검증하였다.

Ⅰ. 서 론

디바이스 핑거프린팅(Device Fingerprinting)은 사용자 기기의 하드웨어 및 소프트웨어 정보를 조합하여 고유한 디지털 지문을 생성하는 기법이다[1]. 핑거프린팅은 사용자 실행 환경 기반의 고유한 식별값(핑거프린트)을 제공하므로 인증 절차의 보조 수단으로 활용되며, 실행 환경 분석을 통해 봇 탐지나 취약한 실행 환경의 식별이 가능하다[2].

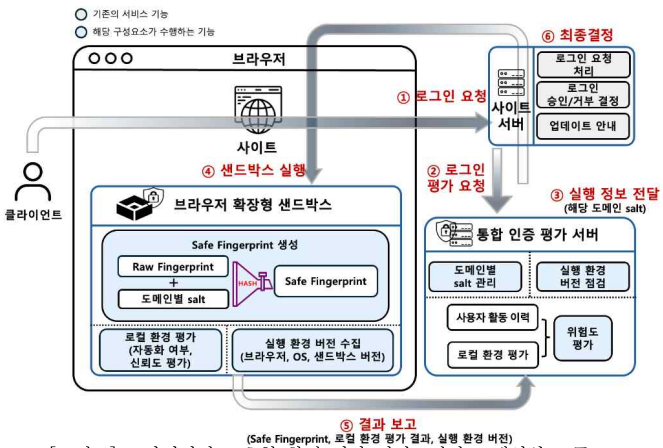
이러한 핑거프린팅 제공업체들은 사용자 기기에 대한 여러 세부 정보들의 집합인 원시 핑거프린트(Raw Fingerprint)를 제공업체 서버로 전송하여 중앙에서 분석 및 관리하는 구조를 주로 사용한다. 이 과정에서 어느 도메인에서든 한 사용자 기기에 대해 항상 동일한 Raw Fingerprint가 수집되고 제공업체 서버의 생성 로직에 따라 일관된 식별값이 부여된다. 그러나 Raw Fingerprint가 제공업체에게 그대로 노출되며, 일관된 식별값으로 인해 도메인간 사용자 활동 추적이 가능해지는 문제가 발생한다.

이러한 배경 속에서 최근 제안된 접근이 프라이버시 보호형 클라이언트 측 핑거프린팅(Privacy-preserving Client-side Fingerprinting, PCF)이다[2]. PCF는 브라우저 내부의 샌드박스에서 Raw Fingerprint를 수집하여 서버로 전달하지 않는다. 또한 각 도메인에 대해 고유하게 부여된 랜덤값인 salt를 이용해 핑거프린트를 해시하여 도메인 단위로만 유효한 안전한 핑거프린트(Safe Fingerprint)를 생성한다. 이로 인해 동일 도메인 내에서의 사용자 식별은 가능해진다. 하지만 Raw Fingerprint에 접근할 수 없게 되므로 봇 탐지나 취약한 실행 환경과 같은 세부 환경 분석에는 한계가 존재한다.

이에, 본 논문에서는 PCF 모델을 확장하여 사용자 식별 기능을 유지하면서도 브라우저 확장형 프로그램을 통해 클라이언트 측 환경평가를 수행함으로써 봇 탐지, 취약한 환경 관리를 지원하는 '프라이버시 보호형 환경 평가 핑거프린팅 프레임워크'를 제안하고 이를 검증한다.

Ⅱ. 프라이버시 보호형 환경 평가 핑거프린팅 프레임워크 구성요소

본 논문의 프레임워크는 [그림 1]과 같이 통합 인증 평가 서버, 브라우저 확장형 샌드박스, 사이트 서버로 구성된다. Raw Fingerprint는 브라우저 확장형 샌드박스 내부에서만 처리되며 외부로 노출되지 않도록 설계되었다. 또한 샌드박스에서 사용자 환경 평가를 수행하여 안전한 로그인 결정을 지원하는 구조를 구현한다.



[그림 1] 프라이버시 보호형 환경 평가 핑거프린팅 프레임워크 구조

2.1 통합 인증 평가 서버

통합 인증 평가 서버는 도메인별 salt 관리, 위험도 평가, 사용자의 실행 환경 버전 점검을 수행한다.

(1) 도메인별 salt 관리

통합 인증 평가 서버는 각 도메인마다 고유한 salt를 생성·관리한다. 해당 salt는 브라우저 확장형 샌드박스에 전달되어 Safe Fingerprint 생성에 사용된다.

(2) 위험도 평가

위험도 평가는 로그인 시도의 위험 징후를 점수로 산출하는 절차이다. 이를 위해 통합 인증 평가 서버는 사용자의 과거 활동 이력과 브라우저 확장형 샌드박스가 제공한 로컬 환경 평가 결과를 핵심 입력으로 활용한다. 이전 로그인 시도에서 수집된 접속 IP·국가·시간 정보와 로컬 환경 평가는 Safe Fingerprint를 기준으로 동일 기기의 기록으로 누적되며, 이를 기반으로 사용자 행동 패턴을 분석한다. 이 과정에서 접속 위치의 변화, 단기간 반복 로그인 시도, 비정상 다계정 사용 징후 등 다양한 행위 기반 신호를 고려하여 위험도를 산출한다. 최종 위험도는 사이트 서버의 로그인 승인 판단에 활용된다.

(3) 사용자의 실행 환경 버전 점검

브라우저 확장형 샌드박스에서 전달받은 사용자의 실행 환경 버전을 통해 브라우저, 운영체제, 브라우저 확장형 샌드박스의 보안 기준을 충족 여부를 점검하고, 구버전 환경인 경우엔 업데이트 필요 여부를 나타내는 플래그를 생성한다.

2.2 브라우저 확장형 샌드박스

브라우저 확장형 샌드박스는 Raw Fingerprint를 외부로 노출하지 않으면서 도메인 단위의 Safe Fingerprint 생성, 로컬 환경 평가, 사용자의 실행 환경 버전 수집을 수행한다.

(1) Safe Fingerprint 생성

Safe Fingerprint 생성은 사용자의 실제 환경 정보를 직접 노출하지 않으면서도 기기를 식별하기 위한 핑거프린트를 만드는 과정이다. 이를 위해 샌드박스는 브라우저 종류 및 버전, 운영체제 정보, CPU 논리 코어 수, 디바이스 메모리, 화면 해상도, 언어 및 시간대 설정 등 실행 환경 정보를 수집해 Raw Fingerprint를 구성한다. 해당 Raw Fingerprint는 통합 인증 평가 서버가 제공한 도메인별 salt와 결합해 해시하여 Safe Fingerprint로 변환된다.

(2) 로컬 환경 평가

로컬 환경 평가는 브라우저 확장형 샌드박스가 사용자의 실행 환경을 직접 진단하여, 로그인 시도가 정상적인 사용자 환경에서 발생했는지를 판단하기 위한 과정이다. 이 평가는 Raw Fingerprint가 외부로 전달되지 않는 상태에서 [표 1]과 같이 클라이언트 측에서 자동화 여부와 환경 신뢰도를 산출함으로써, 통합 인증 평가 서버의 위험도 판단에 필요한 핵심 신호를 제공한다.

[표 1] 로컬 환경 평가 항목

평가 항목	정의	판정 기준
자동화 여부	실행 환경의 자동화 여부를 식별하기 위한 절차	navigator.webdriver 활성화, Headless UA 패턴, 저장소 기능 부재 등 자동화 환경의 주요 지표 기반 판정
신뢰도 평가	실행 환경이 일반적인 사용자 환경과 얼마나 일치하는지를 평가	언어 설정 부재, DNT 활성화, 비정상적인 CPU 코어 수 등 환경 이상 신호를 감점 요소로 활용

(3) 실행 환경 버전 수집

샌드박스는 브라우저, 운영체제, 브라우저 확장형 샌드박스 버전 정보를 수집한다.

2.3 사이트 서버

사이트 서버는 로그인 요청이 발생하면 통합 인증 평가 서버로 로그인 평가를 요청한다. 이후 통합 인증 평가 서버의 분석 결과로 산출된 위험도 점수는 로그인 승인 여부를 판단에 활용되며, 사용자의 실행 환경 버전 점검 결과는 업데이트 안내에 활용될 수 있다.

2.4 프레임워크 동작 흐름

본 논문에서 제안하는 프레임워크는 전체 동작 흐름은 [표 2]와 같이 6단계로 구성된다.

[표 2] 프레임워크 동작 단계별 세부 내용

단계	세부 내용
① 로그인 요청	• 사용자의 로그인 요청이 사이트 서버로 전달
② 로그인 평가 요청	• 사이트 서버는 로그인 승인 여부 판단을 위해 통합 인증 평가 서버에 평가를 요청
③ 실행 정보 전달	• 통합 인증 평가 서버는 해당 도메인 salt를 사이트 서버에 전달 • 사이트 서버는 이를 브라우저 확장형 샌드박스가 사용할 수 있도록 브라우저에 전달
④ 샌드박스 실행	• Raw Fingerprint를 수집하고 전달받은 salt로 Safe Fingerprint를 생성 • 자동화 여부, 신뢰도 점수를 산출하여 로컬 환경 평가 수행 • 실행 환경 버전 정보 수집
⑤ 결과 보고	• 샌드박스는 Safe Fingerprint, 로컬 환경 평가 결과, 실행 환경 버전 정보를 통합 인증 평가 서버에 전달 • 통합 인증 평가 서버는 샌드박스 실행 결과와 사용자 과거 활동 이력을 결합해 위험도를 계산하고 환경의 보안 기준 충족 여부를 평가한 후 결과를 사이트 서버에 전달
⑥ 최종 결정	• 사이트 서버는 전달받은 위험도를 기반으로 로그인 승인 여부를 결정 • 실행 환경이 보안 기준을 충족하지 않을 경우 업데이트 안내 등 추가 조치를 수행

Ⅲ. 프레임워크 구현 검증 결과

본 논문에서 제안한 프레임워크의 도메인별 Safe Fingerprint 생성 여부와 자동화 실행 환경 탐지 기능을 검증하였다. 이를 통해 Raw Fingerprint를 외부로 전송하지 않으면서도, 도메인 단위 사용자 식별과 사용자 환경 평가가 가능함을 확인하였다.

(1) 도메인별 Safe Fingerprint 생성 여부

도메인별 Safe Fingerprint 생성 여부를 검증하기 위해, 두 개의 사이트 서버를 구축하고 동일한 기기로 로그인을 수행하였다. 검증 결과, [그림 2]와 같이 도메인별 salt 적용에 따라 각 사이트에서 생성된 Safe Fingerprint가 서로 다르게 산출됨을 확인하였다.

[그림 2] 도메인별 Safe Fingerprint

(2) 자동화 실행 환경 탐지 기능

자동화 도구(Puppeteer, Playwright)를 이용환 환경에서 로그인을 수행하고 로컬 환경 평가 및 위험도 평가 결과를 분석하였다. 그 결과, 브라우저 확장형 샌드박스의 로컬 환경 평가에서 자동화 여부는 참으로 판정되었으며, 비정상적인 실행 환경 특성을 반영하는 신뢰도 점수는 10으로 낮게 산출되었다. 해당 결과는 통합 인증 평가 서버로 전달되어 높은 위험도를 의미하는 0.85의 위험도 점수를 산출하였다.

Ⅳ. 결론

본 논문에서는 디바이스 핑거프린팅의 프라이버시 문제를 완화하면서도 보안 기능을 유지하기 위해 프라이버시 보호형 환경 평가 핑거프린팅 프레임워크를 설계하고 구현하였다.

제안한 프레임워크는 도메인별 salt를 적용한 Safe Fingerprint를 통해 도메인간 사용자 추적을 방지하며, 브라우저 확장형 샌드박스에서 로컬 환경 평가를 수행한다. 해당 결과는 통합 인증 평가 서버의 위험도 평가에 반영되어 로그인 승인 여부 판단에 활용된다.

본 논문은 Raw Fingerprint를 서버로 전송하지 않으면서도 사용자 식별과 환경 평가를 동시에 수행할 수 있음을 보였다는 점에서 의의가 있으며, 향후에는 다양한 자동화 우회 기법을 고려한 추가 검증을 통해 프레임워크의 적용 범위를 확장할 계획이다.

ACKNOWLEDGMENT

이 논문은 2026년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. RS-2024-00396797, 지능형 오픈랜(Open RAN) 보안 플랫폼 핵심 기술 개발)

참 고 문 헌

[1] Kumar, V., "Device Fingerprinting for Cyber-Physical Systems: A Survey," ACM Computing Surveys, July. 2023.

[2] Fernandez-de-Retana, A., "Keep Your Identity Small: Privacy-preserving Client-side Fingerprinting," Igor Santos-Grueiro HP Labs, Seq. 2023.