IARIA

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

SECURWARE 2024

ALEXANDER LAWALL

Fingerprinting and Tracing Shadows:

The Development and Impact of Browser Fingerprinting on Digital Privacy

Nice, November 2024

PROF. DR. ALEXANDER LAWALL

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Academic Roles

- Program Director, B.Sc. & M.Sc. Cyber Security and Cyber Security Management
- Professor in Cyber Security (Distance & On-site Learning)

Expertise

- System & Network Security
- Web Application & Cloud Security
- IoT and Industrial IT Security

Professional Affiliations

- Leadership Committee, "Management of Information Security" (Society for Informatics, GI)
- Professional Lead, "Security & GRC in IT" (Summit Leipzig)
- Member, Association of Cyber Forensics and Threat Investigators (ACFTI)
- Member, Zentrum Digitalisierung Bayern (ZD.B)

Research & Publications

- Focus Areas: Cyber Security, Information Security, Industry 4.0/5.0, IoT, Rights Management
- Publications in national/international Journals and Conferences
- Keynote Speaker, Program Chair, Panel Expert of International Conferences

AGENDA

MOTIVATION AND RESEARCH QUESTIONS

Motivation

Traditional Method - Cookies

- User consent for traditional cookies as per GDPR (→ sense of control for users)
- Properties: Easy to clear; increasingly restricted; browsers actively blocking or limiting (privacy concerns)

Privacy Concerns with Cookies

- Local data storage with cookies (→ users manage or delete this data)
- Transparency of cookies (→ cookie consent mechanisms for online privacy)

➢ Techniques like browser fingerprinting bypass these controls?! How?

MOTIVATION AND RESEARCH QUESTIONS

Research Questions

RQ1: *What **methods** are used in **browser fingerprinting** and what **user data** are collected in the process?*

RQ2: *How has the **development of browser fingerprinting** as a **user identification method** influenced **user privacy** and **data protection** in the digital space?*

Criteria: *Uniqueness, Stability, and Entropy*

BROWSER FINGERPRINTING

Definition and Usage

- Collects characteristic information from the browser (stealthily in the background)
- Used for tracking users and IT security applications

Comparison with Cookies

- Does not require storing data on the user's computer
- Operates secretly and without user consent

Challenges in Digital Privacy

- Creating a new identity is difficult
- GDPR privacy laws offer little protection

Legal Loopholes

- Not explicitly mentioned in GDPR
- Website operators claim "legitimate interest" for data collection

Source: Created with Microsoft Copilot

BROWSER FINGERPRINTING

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Passive Data Collection

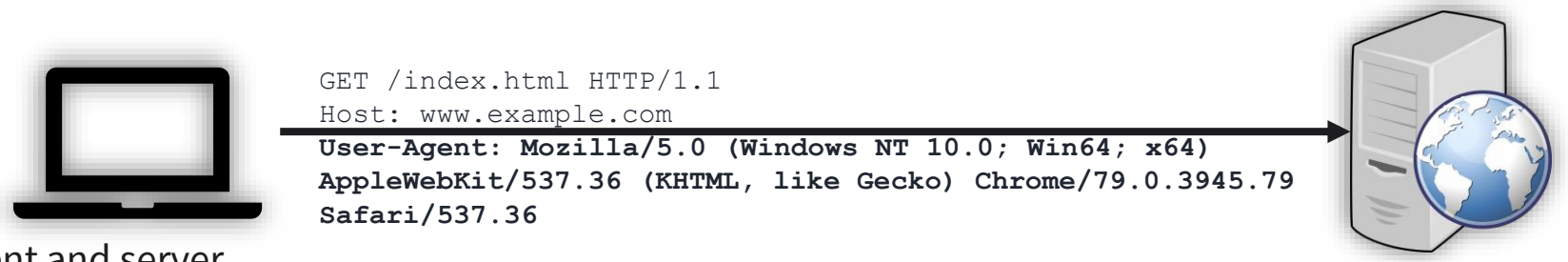
- Transmits information like user's preferred language via HTTP headers
- Provides limited information

Active Data Collection

- Uses JavaScript to gather detailed browser information
- Collects data such as screen resolution, installed add-ons, and graphics card data
- Merges collected data into a unique fingerprint

METHODS OF BROWSER FINGERPRINTING

HTTP Header Attributes



Definition and Basics

- Part of every HTTP request between client and server
- Transmits functional and compatibility-related information
- Based on HTTP version 1.1, with modifications in HTTP/2
- Key fields i.e., User-Agent, Accept, and Content-Language

Analysis

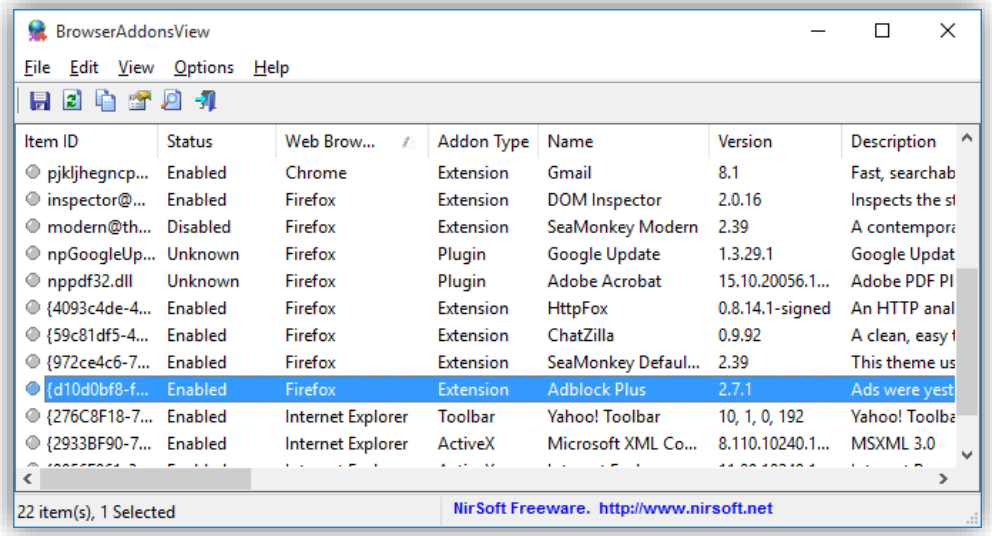
- Attributes differ by browser and version
- Effective fingerprinting requires consistent attributes
- Reliable fields: User-Agent, Accept, Content-Encoding, Content-Language
- User-Agent offers high uniqueness

METHODS OF BROWSER FINGERPRINTING

Enumeration of Browser Plugins

Definition and Basics

- Browser plugins can be preinstalled or user-added
- Indirectly modify most browser features except extensions
- High demand for accurate enumeration of extensions
- Detects system plugins (e.g., PDF viewer) to identify user environments



Source: https://www.nirsoft.net/utils/web_browser_addons_view.html

Analysis

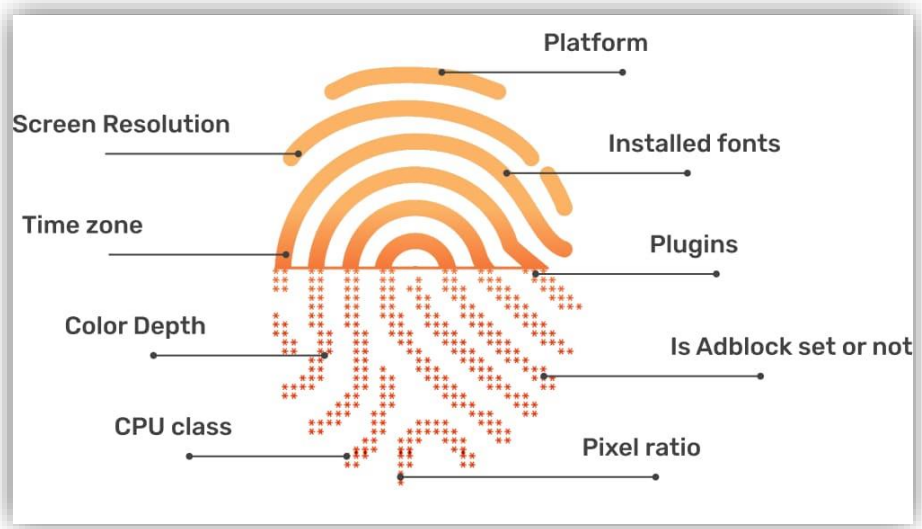
- Information-rich plugins like Flash have disappeared
- Most browsers no longer support NPAPI plugin interface
- Navigator.plugins object shows only standard plugins
- New methods to enumerate extensions have emerged
- Chromium-based browsers can access extension settings via local URL

METHODS OF BROWSER FINGERPRINTING

Canvas Fingerprinting

Definition and Basics

- Uses Canvas element from HTML5
- Generates a unique fingerprint based on hardware and software variations
- Uses the HTML5 Canvas API to render an image and capture unique graphic handling



Source: https://gologin.com/de/blog/what-is-canvas-fingerprinting/

Analysis

- Script draws a hidden 2D graphic
- Uses fonts and sizes to test uniqueness
- Image data hashed and sent to server
- Enables system profiling
- Variances in hardware/software produce distinct rendering outputs

METHODS OF BROWSER FINGERPRINTING

Web Graphics Library (WebGL) Fingerprinting

Source: Created with Microsoft Copilot

Definition and Basics

- Uses WebGL JavaScript API based on OpenGL ES 2.0
- Renders 2D and 3D graphics with high performance
- Captures unique hardware information, especially about the graphics processor

Analysis

- Uses a Canvas element to access the API
- Collects data without user interaction
- Browsers like WebKit and Firefox mask specific hardware details to protect privacy
- Accesses variables for graphics details, providing a stable fingerprint

METHODS OF BROWSER FINGERPRINTING

Audio Fingerprinting

Definition and Basics

- Web Audio API processes and synthesizes audio signals in browsers
- Identifies systems through hardware differences
- Analyzes signal processing characteristics for fingerprinting

Analysis

- Involves acoustic measurements for unique device fingerprint
- Uses AudioContext, AudioBuffer, Oscillator, and Compressor
- Dynamic Compressor (DC) method is highly stable
- Fast Fourier Transform (FFT) converts signals from time to frequency domain
- DC and FFT often used together for reliability

Source: https://www.reddit.com/r/programming/comments/mb0ob8/how_the_web_audio_api_is_used_for_browser/

METHODS OF BROWSER FINGERPRINTING

Font Fingerprinting

Definition and Basics

- Identifies devices by recognizing installed fonts
- Creates unique digital fingerprints for tracking and identification

Analysis

- Post-Adobe Flash, JavaScript uses fallback mechanisms for font recognition
- Invisible div elements and canvas elements identify installed fonts
- Local Font Access API requires user consent, not suitable for fingerprinting

Source: Created with Microsoft Copilot

METHODS OF BROWSER FINGERPRINTING

Screen Fingerprinting

Source: Created with Microsoft Copilot

Definition and Basics

- Identifies a device by analyzing screen-related characteristics
- Includes screen resolution, pixel depth, color depth, and browser window size
- Leverages uniqueness of screen configurations and browser modifications

Analysis

- JavaScript provides attributes for screen and browser window characteristics
- Details include color depth, screen orientation, and screen dimensions
- Values like window.innerWidth and window.innerHeight determine browser window’s inner area

METHODS OF BROWSER FINGERPRINTING

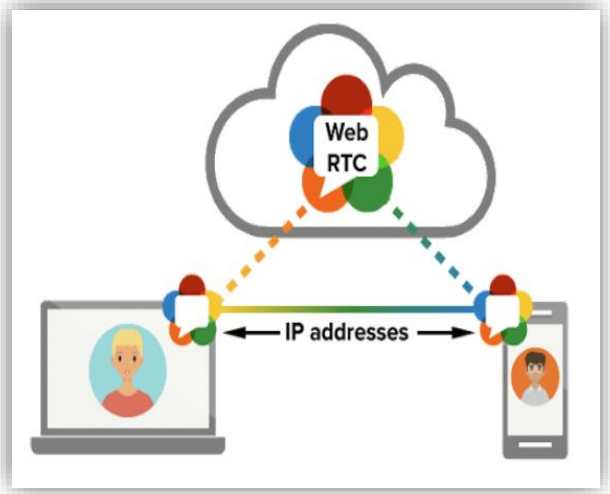
Web Real-Time Communication (WebRTC) Fingerprinting

Definition and Basics

- WebRTC is a JavaScript interface in most browsers
- Facilitates real-time communication over HTTP
- Reveals private and public IP addresses
- Provides information about connected devices

Analysis

- No permissions required for establishing WebRTC connections
- IP addresses can be read from RTCPeerConnection object
- Can enumerate local network to build unique profiles
- DetectRTC project demonstrates WebRTC's capabilities



Source: https://www.tonmind.com/blog/webrtc-web-real-time-communication_b21

METHODS OF BROWSER FINGERPRINTING

CSS Fingerprinting

Definition and Basics

- Passive method using CSS, unlike active JavaScript techniques
- CSS enhances HTML presentation with selectors and filters

Source: Created with Microsoft Copilot

Analysis

- Pre-2010: :visited selector detected visited sites via link color
- Post-2010: Time-based methods required JavaScript, impractical
- 2015: Takei et al. (2015) introduced JavaScript-free method using CSS properties and @media queries

METHODS OF BROWSER FINGERPRINTING

Additional JavaScript Attributes

Definition and Basics

- JavaScript used to extract information from interfaces
- Techniques share characteristics with other JavaScript-based methods

Analysis

- Navigator object provides various information
- JavaScript implementation varies between browsers
- Differences in function availability and execution
- getClientRects function used for precise DOM element data

```
// Funktion zum Abrufen von Browser-Attributen
function getBrowserAttributes() {
    const attributes = {
        screenResolution: `${window.screen.width}x${window.screen.height}`,
        colorDepth: window.screen.colorDepth,
        userAgent: navigator.userAgent,
        language: navigator.language,
        platform: navigator.platform,
        cookiesEnabled: navigator.cookieEnabled,
        javaEnabled: navigator.javaEnabled(),
        onlineStatus: navigator.onLine,
        timezone: Intl.DateTimeFormat().resolvedOptions().timeZone,
        hardwareConcurrency: navigator.hardwareConcurrency,
        deviceMemory: navigator.deviceMemory,
        maxTouchPoints: navigator.maxTouchPoints,
        vendor: navigator.vendor,
        product: navigator.product,
        appName: navigator.appName,
        appVersion: navigator.appVersion,
        appCodeName: navigator.appCodeName,
        productSub: navigator.productSub,
        vendorSub: navigator.vendorSub
    };
    return attributes;
}

// Beispielverwendung
const browserAttributes = getBrowserAttributes();
console.log(browserAttributes);
```

Source: Created with Microsoft Copilot

METHODS OF BROWSER FINGERPRINTING

Advanced Techniques Using Machine Learning

Definition and Basics

- JavaScript gathers hardware and software information
- Side-channels capture behavioral differences
- Methods include plugin enumeration, font fingerprinting, and CSS fingerprinting

Analysis

- Wang et al. (2021) used cache, memory, and CPU activity to identify websites
- CSS selectors previously revealed browsing history
- Machine learning models categorize results with 80-90% accuracy
- Potential future implementations with WebAssembly and Performance API

Source: Created with Microsoft Copilot

METHODS OF BROWSER FINGERPRINTING

Aggregated Results of the Analysis

Fingerprinting Method	Uniqueness	Stability	Entropy	Impact on User Privacy	Defense Techniques
HTTP Header Attributes	Low	Moderate	Low	Moderate impact: limited detail but useful when combined with other methods.	Altering or masking headers (e.g., randomizing User-Agent).
Enumeration of Browser Plugins	Moderate	High	High	High impact: reveals sensitive data, such as installed plugins.	Disabling plugin enumeration, avoiding unnecessary add-ons.
Canvas Fingerprinting	High	Moderate	High	High impact: generates unique fingerprints based on rendering.	CanvasBlocker extension to block or manipulate rendering.
WebGL Fingerprinting	High	High	High	High impact: collects detailed hardware data for tracking.	Block or manipulate WebGL outputs.
Audio Fingerprinting	Moderate	High	Moderate	High impact: captures unique audio processing details.	Disable Web Audio API, use privacy extensions.
Font Fingerprinting	High	High	Moderate	High impact: identifies installed fonts, making it persistent.	Limit font access with privacy-focused browsers (e.g., Tor).
Screen Fingerprinting	Moderate	High	Low	Moderate impact: uses screen resolution and window size but less effective on mobile devices.	Fix window size or limit resolution reporting with privacy browsers.
WebRTC Fingerprinting	Very High	High	Very High	Very high impact: exposes real IP addresses, even behind VPNs.	Disable WebRTC, use extensions that block data collection.
CSS Fingerprinting	Low	Moderate	Low	Low impact: provides limited system and style information.	Limit or disable CSS fingerprinting through extensions or scripts.
JavaScript Attributes	Moderate	High	Moderate	Moderate impact: uses various browser features for tracking.	Disable unnecessary JavaScript functions or use privacy extensions.
Advanced Machine Learning Fingerprinting	Very High	Very High	Very High	Very high impact: uses side-channel data (e.g., CPU/cache) for tracking.	Limit access to Performance API and WebAssembly, emerging defenses needed.

CONCLUSION

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Summary

Browser Fingerprinting

- Growing technique in online tracking
- Identifies and tracks users without cookies
- Uses device, software, and behavioral attributes

Privacy and Security

- Raises significant privacy concerns
- Limited user control and consent
- Valuable for advertisers and security

Regulatory and Anti-Fingerprinting Efforts

- GDPR and other privacy laws lack specific fingerprinting guidelines
- Enforcement is inconsistent

Implications for Practice

Consent and Cookies

- Accept only necessary cookies in banners
- Regularly delete cookies to prevent tracking
- Important for news sites to avoid misuse of data

Blending in with the Masses

- Reducing APIs and data sources can make users more identifiable
- Use widely adopted browsers and protection mechanisms

Browser Choice

- iOS: Safari for advanced tracking protection
- Android: Mull browser for fingerprinting protection, Brave as an alternative
- Desktops: Brave, Librewolf, and Mullvad for privacy features

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

What are your opinions on Browser Fingerprinting: Concerns for Digital Privacy or a tool for enhancing security?

What do you think about Automatic Content Recognition used in Smart TVs and Smartphones?

Prof. Dr. Alexander Lawall
alexander.lawall@iu.org