BÁNKI KÖZLEMÉNYEK
3. ÉVFOLYAM 1. SZÁM

General characteristics of Android browsers with focus on security and privacy features

Petar Čisar*, Sanja Maravic Cisar**, Igor Fürstner***
Academy of Criminalistic and Police Studies, Belgrade, Serbia,
**Subotica Tech, Subotica, Serbia,
***Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Budapest, Hungary,
petar.cisar@kpa.edu.rs, sanjam@vts.su.ac.rs, furstner.igor@bgk.uni-obuda.hu

***Abstract* —Satisfactory level of security in the use of the Internet in mobile devices depends on several factors. One of them is safe browsing. A key factor in providing secure browsing is the application of a browser with the appropriate methods applied: clearing cookies, cache and history, ability of incognito browsing, using of whitelists and encryptions and others. This paper presents an overview of the various security and privacy features used in the most frequently used Android browsers. Also, in the case of several browsers and types of mobile devices, the use of benchmark tests is shown. Bearing in mind the differences, when choosing a browser, special attention should be paid to the applied security and privacy features.**

Keywords: Android browser, security, adblock, tracking, encryption, benchmark test

1 INTRODUCTION

The increased use of mobile devices to store large amounts of data also carries a risk of loss or theft, which can compromise the security of information. In order to minimize the risks of such abuses, mobile and wireless users need to be aware of security issues relating to the technology [1]. One of the factors that significantly affects the level of security in the use of mobile devices is browser [2]-[4]. Safe browsing concept protects users against Internet security threats by allowing applications to check URLs against lists of unsafe web resources, such as social engineering sites (phishing and deceptive sites), and sites that host PHAs (Potentially Harmful Applications) or unwanted software. When users attempt to visit an unsafe web resource, their safe browsing-supported browser displays a warning. There are a large number of browsers on the market with very different security features. Before installing one of them, it is useful to first know their capabilities and compare them with each other [5]-[8].

Android browsers use different security features (general overview):

- Using website whitelists - list of items (e-mail addresses or domain names) from which a blocking program (spam filter) will allow messages to be received. When a whitelist is used, all entities are denied access, except those included in the whitelist.
- Possibility of clearing cookies, cache, and granular history (no passwords, no cookies, no trackers).
- Blocking or allowing trackers.
- Adblocker - user can block pop-ups, advertisements, banners & ad-videos.
- Incognito browsing mode - offers real private browsing experience without leaving any historical data.
- Using of HTTPS protocol - enforces SSL (Secure Socket Layer) security protocol (using of certificates) wherever that's possible.
- Disabling features like JavaScript, DOM (Document Object Model) storage
- Using fingerprinting techniques

Further sections of this paper provide an overview of the applied security and privacy methods for more popular Android browsers. Also, in order to compare the adequate features of browsers, the use of benchmark tests on different mobile devices will be shown.

2 SECURITY AND PRIVACY FEATURES OF DIFFERENT ANDROID BROWSERS

This chapter provides an overview of most important security features of a large number of popular Android browsers.

Ghostery [9]

- Provides an instant overview of the trackers on each visited site, then block or allow them.
- Manage website whitelists.
- Largest tracker database - with over 2200 trackers and 4500 scripts.
- Additional privacy options with quick and easy access to clear cookies, cache, and granular history.

Dolphin Zero [10]

- *Adblock* is one of the best adblock-browser.
- Incognito browsing.
- Clean UI (user interface) and fast navigation - user can add most visited websites as speed dial icons with a friendly UI and one-touch access.

That includes theming (theming consists of changing the user interface without changing the application logic), flash support, ad-block, incognito mode, and some tertiary features like gesture controls. There is also optional add-on and extension support.

Firefox Focus [11]

- Blocks a wide range of common Web trackers without any settings to set.
- Erases user's history.
- By removing trackers and ads, Web pages may require fewer data and load faster.

This is a security-focused browser application. Basically, every session is in privacy mode. Some features include a one-tap history deletion process, a fairly decent ad-block, and it blocks most types of web trackers.

Firefox [12]

Private browsing mode with added tracking protection - stops ads that track and follow user around the Internet. Browsing history will not be remembered or cookies saved after the action.

Frost Incognito Browser [13]

- Tabbed browsing - Fast, full featured tabbed browser with HTML 5 video support, popup blocker, and user agent switching.
- Ad blocking - Built in ad blocker speeds up page loading and reduces data usage.
- Privacy protection - Automatically clears all browsing history when closing the application.
- Image & bookmark vault - Download images from the web and save bookmarks into a hidden, password protected vault.
- Import & export images - Import or export pictures between device storage and image vault.
- Complete stealth - Frost looks and functions like any other normal browser, until user enter his password into the address bar, which reveals image and bookmark vaults.
- Vault protection - The contents of vaults is hidden from other applications (for instance, gallery or camera) and not viewable when connected to a computer.

Privacy Browser [14]

This browser protects the privacy by disabling features like JavaScript, DOM (Document Object Model) storage, and cookies that are used by websites to track users. Settings can be adjusted by domain and on-the-fly to enable these features when needed. In addition, the browser incorporates the EasyList block lists, which block many tracking technologies even when JavaScript is enabled.

Security and privacy features:

- TOR (The Onion Router) Orbot proxy support
- SSL certificate pinning
- Full screen browsing mode
- Night mode

Krypton [15]

- Privacy - History, cookies and site data are never stored on disk, and never transmitted.
- Security - Each tab is isolated in a separate OS process. Every tab is treated as a distinct instance, with its own memory storage and state.
- Anonymity - Enable TOR with a single tap to hide the IP, avoid surveillance, and circumvent censorship. Includes HTTPS Everywhere (enforces SSL security wherever that's possible), and mitigates common fingerprinting techniques.

Javelin [16]

- Ad block - web browsing with no ads.
- Always incognito - The web history is never saved, and cookies are always deleted. No one needs to know someone's surfing habits.
- Password protected - Prevent any snooping on recent browsing activity, even if it is still active in recently opened applications. Only the user can open the browser.

CM Secure [17]

- Fraud prevention - Warns when browsing potentially fraudulent or malicious websites.
- Malicious download protection - Scans apk file downloads for malware, keeping the device secure.
- User agent - Supports user agent switching to access desktop sites.

Chrome [18]

- Privacy – use incognito mode to browse without saving the history.
- Do Not Track feature - Chrome will automatically send a Do Not Track request with the browsing traffic.
- Safe browsing technology - showing a warning on screen if user tries and navigates to a page which it deems to be unsafe.
- Autofill and payments - Given it pre-populates addresses and credit card details on applications and websites, someone with access to user's phone could not only steal his identity but also rack up a significant amount of spending before he realize something is wrong.
- Setting of site permissions
- Managing user's syncing options
- Disabling sending of (security) reports to Google
- Disabling prediction services (suggestion of search terms and websites)

InBrowser [19]

- No data is saved.
- TOR support via Orbot.
- Supports agent cloaking (no more mobile version of sites).
- Deep integration with LastPass.

Asus Browser [20]

- Lightning speeds - ASUS Browser runs on leading Chrome-based engine to load web pages rapidly.
- Adapts to a region - The Navigation panel displays the popular websites according to user's location.
- Secure Browsing - Built-in security features protect from malware and phishing sites.
- Do-It-Later - Mark pages as a task to be read later when convenient.
- Import bookmarks - Import saved pages in Google Chrome to user's browser.

Puffin [21]

- Puffin speeds up mobile browsing by shifting the workload from the resource-limited devices to the cloud servers.
- It's safe to use public non-secure WiFi through Puffin, but not safe at all for most browsers.
- Puffin uses a proprietary compression algorithm to transmit web data to device, and it can save up to 90% of bandwidth on regular web browsing.

Brave [22]

- Built-in adblock

- Blocks pop-ups
- Battery optimization
- Data optimization
- Tracking protection
- HTTPS Everywhere (for security)

There is an ad blocker built-in. Additionally, it can block third party cookies, block scripts, and it has HTTPS everywhere. Included is per-site settings just in case user need that. It also boasts optimizations for speed and battery life improvements. It also has most of the basic features like bookmarks, history, and a privacy (incognito) mode.

IceCat Mobile [23]

Privacy protection features:

- LibreJS: GNU LibreJS aims to address the JavaScript problem
- HTTPS-Everywhere: Extension that encrypts the communications with many major websites, making browsing more secure.
- SpyBlock: Blocks privacy trackers while in normal browsing mode, and all third-party requests when in private browsing mode. Based on Adblock Plus.
- Fingerprinting countermeasures: Fingerprinting is a series of techniques allowing to uniquely identify a browser based on specific characteristics of that particular instance (like what fonts are available in that machine). Unlike cookies the user cannot opt-out of being tracked this way, so the browser has to avoid giving away that kind of hints.

Orbot [24]

TOR (free software for enabling anonymous communication) is available for Android by installing the package named Orbot.

Orbot is an application that allows mobile phone users to access the web, instant messaging and email without being monitored or blocked by their mobile internet service provider. Orbot brings the features and functionality of Tor to the Android mobile operating system.

Orbot contains Tor and *libevent* (asynchronous event notification software library). Orbot provides a local HTTP proxy and the standard SOCKS4A/SOCKS5 proxy interfaces into the Tor network. Orbot has the ability to transparently torify all of the TCP traffic on user's Android device when it has the correct permissions and system libraries.

Orbot is a free proxy app that empowers other apps to use the internet more securely. Orbot uses Tor to encrypt Internet traffic and then hides it by bouncing through a series of computers around the world. Tor is free software and an open network that helps defending against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.

Opera Mini [25]

- Keeps advertisements away - can be very frustrating at times. They slow down web pages, redirect users to other pages and if there is a video involved, they waste mobile data without the user's knowledge. Opera Mini is the only mobile browser which has a built-in ad blocker. It is very effective and can block all banner or video ads on any webpage from showing on the browser.
- Allows video download - video downloading allows users to download videos uploaded on social media networks such as Facebook, Twitter or other web pages in MP4 file formats.
- Reduces stress on eyes - Several studies have pointed out that the blue light from smart phones not only affects eyes, but also disrupts sleep and can lead to obesity, cardiovascular diseases and metabolic disruption. Opera Mini has this unique night mode which blocks the blue light by switching on a more soothing pink colored screen instead of the sharp looking white.
- Stream videos faster - Video boost is another video-related tool in opera Mini, which reduces buffering time for videos by reducing the size of the video data. This feature allows users to stream video on any online streaming site such as Netflix or YouTube with zero lags.
- Data saver mode - the technology to compress and convert a web page and its contents into format which uses less bandwidth and open a lot faster. The extreme data saver mode is an improved version of it, which can save up to 90% of mobile data.

Epic [26]

Based on Chromium, this browser implements a large number of features to maximize privacy. Cookies and trackers are eliminated after each session, all searches are proxied through the firm's own servers (which means there is no way to connect an IP address to a search), and it attempts to prioritize SSL connections wherever possible - useful for open Wi-Fi connections. It does not collect data about its users and comes with excellent built-in ad blocking.

For a fully encrypted connection, it includes a one-button proxying feature that does slow down browsing but will appeal to some users.

3 ANDROID BROWSERS BENCHMARK TESTS

In order to compare the browsers' characteristics, appropriate benchmark tests are used. There are numerous different tests, which differ in their capabilities. For instance: Sunspider-1.0.2, Dromaeo (Javascript performance testing), Qualys Browsercheck, Basemark's browser benchmark - Web 3.0, Mozilla Kraken Javascript Benchmark v 1.1 and AnTuTu Benchmark v7. The results of Mozilla Kraken Javascript Benchmark are shown in Fig. 1.

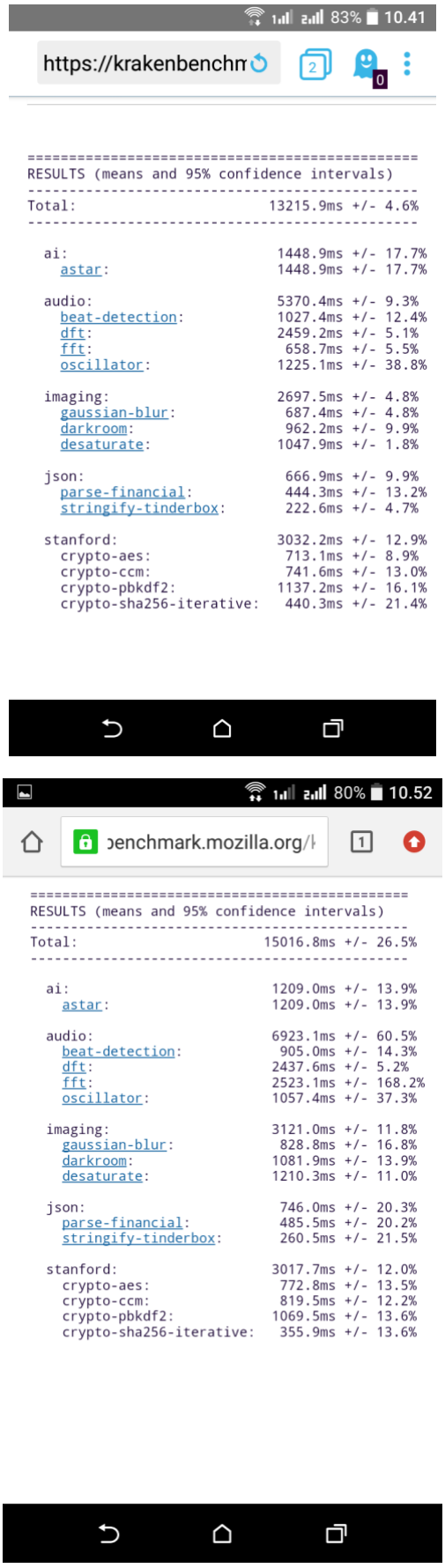

Fig. 1. Mozilla Kraken Javascript Benchmark (used mobile device HTC Desire 630) [27]

Test results - total for the following browsers (mobile device HTC Desire 630): Ghostery - 13215.9 ms, Firefox Focus - 12553.6 ms and Chrome - 15016.8 ms.

Test result - total for the Chrome browser (mobile device Samsung Galaxy J5 2016): 15842.4 ms.

For instance, AnTuTu Benchmark v7 [28], HTML5 Test (web browser performance (speed and compatibility) include JavaScript, Layout, CSS, SVG, Canvas test, Game test) is shown in Fig.2.

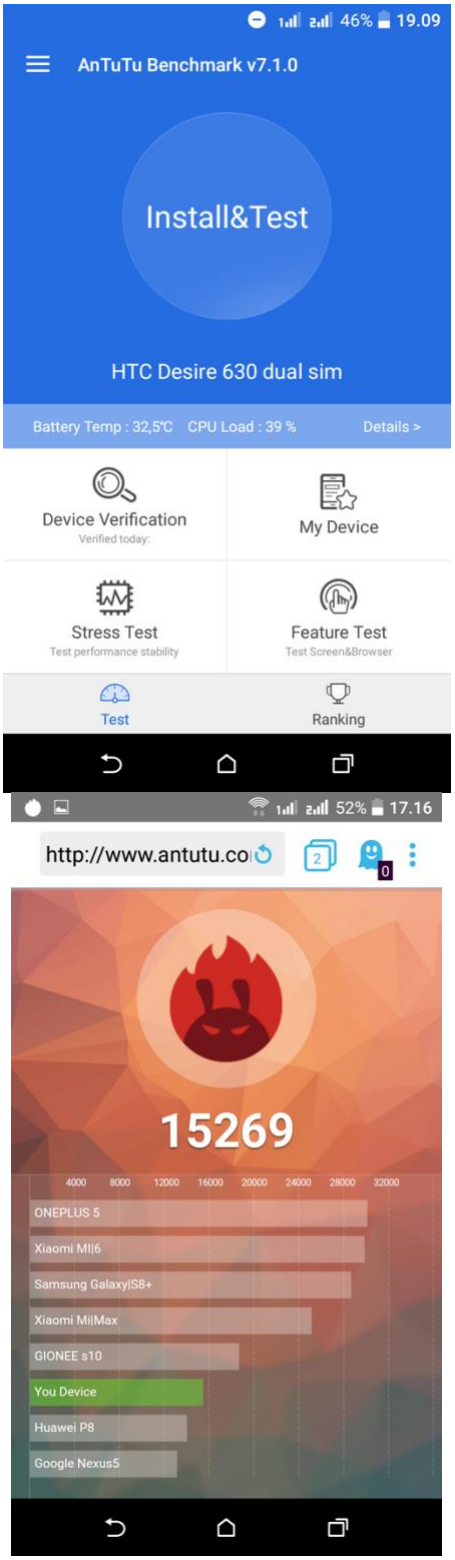

Fig. 2. HTML5 test (AnTuTu, used mobile device HTC Desire 630)

Test results (overall benchmark scores) for the following browsers (mobile device HTC Desire 630): Ghostery - 15269, Firefox Focus - 15800 and Chrome - 16605.

Test results for the following browsers (mobile device Samsung Galaxy J5 2016): Opera - 14695, Firefox - 3016 and Chrome - 12704.

Some other comparison of Android browsers (Firefox Quantum, Samsung Internet, Brave Browser, Microsoft Edge and Google Quantum) is given in Fig. 3:

- Browser Engine - The foundation of the browser which determines basic functionality and overall speed. Firefox is the only one in the list that uses a different engine, which makes it the only browser that's fundamentally unique. Both Blink and Gecko have similar performance and functionality.
- Basemark Score - A numerical comparison of each browser's performance (benchmarking). Basemark's browser benchmark was run on three different devices and averaged the scores.

Best Android Internet Browsers

GADGET HACKS	Firefox Quantum	Samsung Internet	Brave Browser	Micrsoft Edge	Google Chrome
Browser Engine	Gecko	Blink	Blink	Blink	Blink
Basemark Score	162.86	142.40	215.36	199.08	204.03
Features					
Sync Across Devices	Yes	Yes	No	Yes	Yes
Tab Swiping	No	Yes	Yes	Yes	Yes
Touch to Search	No	Yes	No	No	Yes
Beta Version Available	Yes	Yes	No	Yes	Yes
Data Saving Mode	No	No	No	No	Yes
Themes	Yes	No	No	No	No
Dark Mode	No	Yes	No	Yes	No
Reading Mode	Yes	No	No	Yes	No
Progressive Web Apps	Yes	Yes	Yes	Yes	Yes
Security					
Private Browsing	Yes	Yes	Yes	Yes	Yes
Ad Blocker	Yes	Yes	Yes	Yes (Beta)	No
Tracking Protection	Yes	Yes	Yes	No	No
Extensions	Yes	Yes	No	No	No
Password Manager	Yes	Yes	Yes	Yes	Yes

Fig. 3. Comparison of Android browsers [29]

4 General Features

Modern mobile browsers have many practical features that enable comfortable operation:

- Sync across devices - The ability to share data such as history, bookmarks, and saved logins across multiple devices, including desktops, tablets, and other smartphones. Syncing requires logging into the same browser on other device(s).
- Tab swiping - The ability to swipe horizontally on the address bar to navigate between open tabs.
- Touch to search - Selecting text will bring up the search engine along the bottom of display, allowing user to search without ever having to leave the current webpage.
- Data saving mode - Manual control over the reduction of data usage. When enabled, websites are compressed before downloaded by users.
- Themes - The ability to customize the look and design of the browser.
- Dark mode - When turned on, all major elements of the browser will become black or dark grey. Ideal for AMOLED (Active Matrix Organic Light Emitting Diodes) displays and night browsing.
- Reading mode - This feature adjusts the website for an improved reading experience on mobile. Text better matches the display size and ads are removed.
- Progressive Web applications - Websites with the ability to operate as a mobile application. These apps have access to many sensors built into most smartphones, use similar styling, and designed for touch screens. Besides the websites including support, the browser must also support this feature, allowing the user to add the site to home screen for independent operation.

5 Security Features

In order to ensure a higher level of security in the use of network connections, different features are used. For instance:

- Private browsing - The ability to browse the web secretly, without data saving and syncing across devices. Browsing history and logins are not recorded while using this mode.
- Ad blocker - The ability to blocks ads in web pages, either natively or with an extension.
- Tracking protection - Trackers are used by corporations to gather information (such as device info, time, and type of browser) about the user when visiting their website. This feature blocks these trackers, which use cookies to record this information.
- Extensions - The ability to add extra features to the browser by installing miniature programs which enhance browsing experiences.
- Password manager - The ability to store password information to autofill frequently visited websites.

CONCLUSIONS

General security in the use of the Internet in mobile devices mostly depends on the use of adequate browsers. Therefore, when choosing a browser, special attention should be paid to the applied security features. Some of them are of particular importance: private browsing, ad blocker, blocking trackers, using of HTTPS protocol and so on. When choosing, it is recommended to check a specific browser with some benchmarking program, as in this way user get a complete picture of its features.

REFERENCES

[1] Urbas, G., & Krone, T. (2006). Mobile and wireless technologies: security and risk factors, Trends & Issues in Crime and Criminal Justice, No. 329, Australian Institute of Criminology. Available from: https://www.researchgate.net/publication/256088649_Mobile_and_wireless_technologies_security_and_risk_factors [accessed May 18 2019].

[2] Androulidakis, I. (2016). Mobile Phone Security and Forensics: A Practical Approach, Springer. Doi: 10.1007/978-3-319-29742-2

[3] Doherty, J. (2015). Wireless and Mobile Device Security, Jones & Bartlett Learning, 1 edition

[4] Bergman, N., Stanfield, M., Rouse, J., & Scramblay, J. (2013). Hacking Exposed Mobile: Security Secrets & Solutions, 1st Edition, McGraw-Hill Education.

[5] Amrutkar, C., Singh, K., Verma, A., & Traynor, P. (2012). VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security, International Conference on Information Systems Security ICISS 2012, pp. 16-34

[6] Amrutkar, C., van Oorschot, P.C., & Traynor, P. (2011). An Empirical Evaluation of Security Indicators in Mobile Web Browsers. Georgia Tech Technical Report GT-CS-11-10

[7] Terada, T. (2014). Attacking Android browsers via intent scheme URLs, Whitepaper, Mitsui Bussan Secure Directions, Inc. Available from: https://www.mbsd.jp/Whitepaper/IntentScheme.pdf [accessed May 18 2019].

[8] Virvilis, N., Myolonas, A., Tsalis, N., & Gritzalis, D. (2015). Security Busters: Web Browser security vs. rogue sites, Computers & Security, No. 52, Available from: https://www.infosec.aueb.gr/Publications/C&S-Insecure-Browsing.pdf [accessed May 18 2019].

[9] https://www.ghostery.com

[10] https://dolphin.com

[11] https://blog.mozilla.org/blog/2016/11/17/introducing-firefox-focus-a-free-fast-and-easy-to-use-private-browser-for-ios/

[12] https://www.mozilla.org/sr/firefox/mobile/

[13] https://www.crowbarsolutions.com/projects/frost-browser-for-android/

[14] https://www.stoutner.com/privacy-browser/

[15] https://en.apksum.com/developer?dev=Kr36 LLC

[16] https://javelinbrowser.com

[17] https://www.cmcm.com/

[18] https://www.google.com/chrome

[19] https://www.inbrowserapp.com/

[20] https://www.apkmirror.com/apk/zenui-asus-computer-inc/asus-browser/

[21] https://www.puffin.com/android/

[22] https://brave.com

[23] https://www.gnu.org/software/gnuzilla/

[24] https://2019.www.torproject.org/docs/android.html.en

[25] https://www.opera.com

[26] https://www.epicbrowser.com/

[27] https://krakenbenchmark.mozilla.org/

[28] https://www.antutu.com/en/

[29] Gadget Hacks, https://android.gadgethacks.com/how-to/comparing-5-best-internet-browsers-for-android-0181493/