D3.12

Summary report of all FSTP calls

NGI Mobifree

NGI MOBIFREE is made possible with financial support from the European Commission's **Next Generation Internet** programme, under the aegis of **DG Communications Networks, Content and Technology**.

Coordinator

/e/ Foundation
mobifree.org

Open calls main page:
nlnet.nl/mobifree

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101135795.

NGI MOBIFREE

NGI Mobifree

Report on open call subgranting

Coordinator
/e/ foundation
www.mobifree.eu

Project co-funded by the European Commission

NGI NGI Mobifree is made possible with financial support from the European Commission's **Next Generation Internet** programme, under the aegis of **DG Communications Networks, Content and Technology**.

	Dissemination level	
PU	Public	☑
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101135795.

NGI MOBIFREE

Table of Contents

Introduction

The background to the development of NGI Mobifree project is the current mainstream mobile software ecosystem. This ecosystem is dominated by a small number of proprietary technologies by actors which are known for collecting large amounts of data on users. They are closed source and use proprietary formats and protocols, resulting in user lock-in and monopolisation of the markets. NGI Mobifree wants to contribute to the establishment of a more fair mobile software ecosystem which is pro-privacy and pro-openness, applying free and open source principles and using open data and standards, contributing to digital sovereignty of Europeans. NGI Mobifree brings together a number of European organisations in this area to further develop Next Generation Internet (NGI) technologies to realize this.

The ambition of NGI Mobifree is to support the digital sovereignty of European citizens and organizations by further developing open source software that is human-centred and ethical, and by strengthening the ecosystem that provides these software solutions. The broader objective of NGI Mobifree is to scale up mobile software technologies in all four key areas of the mobile software ecosystem through co-creation and piloting with four key sectors of end-users, in order to improve the quality, privacy and openness of these software solutions, and create new business opportunities.

During the review of the outcomes of the open calls held within NGI Mobifree during the first reporting period, the reviewers indicated that they were interested in additional background informatoin on the selection of projects, and how they interact with the NGI Mobifree goals.

In addition to the full project descriptions which are available on the overview page of projects (and which are included as an Annexe to this document for convenience), we have clustered the projects together with a description of why they are a good fit with the programme and how they interacts with the Mobifree goals.

How projects from the Open calls are linked

Mobifree is a programme to boost the development of human-centred and ethical mobile software, and expand the ecosystem of partners working on such software. Part of the effort is a series of open calls that redistribute part of the budget to independent effort, so called **Financial Support to Third Parties** (FSTP). The following IT areas are of particular interest to NGI Mobifree:

- /e/OS, a fully-open-source operating system (OS) for Android-based phones
- Online Workspace / Cloud
- App stores
- Mobile Device Management (MDM)
- Messaging
- Maps
- Disaster & emergency response

These topics are clearly reflected in the topics of the granted projects. The first and largest cluster of projects is concerned with the **security** of /e/OS and other Android operating systems and their app ecosystem. This kind of ***horizontal effort*** to protect the **integrity** of the operating system, find and remove stalkerware, tracking software and detect other malicious activity, is something that is systematically above the responsibility of the individual developer and user. At the same time the incentives for private companies point the other direction: abusing the trust of users can generate a lot of profit. It is therefore a critical issue to address for the open source ecosystem.

Androguard and **OWASP blint** perform static and dynamic analysis of Android apps, analysing the binaries to find malware indicators and generate a **Software Bill of Materials** that can be used to understand inherent weaknesses such as outdated dependencies. **APKpatcher/PyAxml** are tools which can be used to subsequently modify Android package files to remove undesired elements.

Pithus, the **PiRogue Tool Suite**, **Bugbane** and **IsMyPhonePwned** are all tools for mobile device forensic analysis and threat intelligence with different approaches and security guarantees - from 'first aid' approaches like an end-user friendly scanning from a web browser (**IsMyPhonePwned**) or an installable app (**Bugbane**) to more professional analysis tools that perform the analysis externally (**Androguard**, **Pithus**, **PiRogue Tool Suite**) – to avoid the situations where an advanced attacker that has successfully entered a device anticipates such entry level scans and fools the scanner. Obviously, the more professional tools are important building blocks for **Mobile Device Management** at an organisational level.

Projects involved in this cluster

Androguard: *Static and dynamic analysis of Android apps*

APKpatcher/PyAxml: *Support tool to manipulate APK and AXML file*

Bugbane: *App for self-conducting device forensics on Android devices*

IsMyPhonePwned: *Scan phone security directly from a web browser*

OWASP blint: *Versatile binary linter, malware research tool and SBOM generator*

Pithus: *Free and open-source mobile threat intelligence*

PiRogue Tool Suite: *Consensual mobile device forensic analysis and incident response solution*

Another cluster of projects is aimed at improving the ***operating system level*** of /e/OS and other Android operating systems. **Android translation layer (ATL)** allows to run Android apps on Linux, which broadens the utility, enables reuse and makes it much easier for developers to do quality assurance. **VirtuAndroid** is an application-layer virtualisation for Android apps. **SIMcurity** is a highly advanced project to secure how the software handles dealing with a specific piece of cricical hardware in phones, namely the SIM interface. It is well-known that the low level baseband interaction with the SIM card (which is really a small computer) is one of the headache dossiers of security,

and this isolation layer will help protect phones and users against SIM vulnerabilities and hostility. **VoWiFi Watchdog** warns users for misconfigurations and hidden blocks at the mobile telecom provider level, in particular for voice calls ("voice over WiFi"). Without this project, users are likely to blame their open source operating system for intentional and non-intentional breakage by their mobile operator. A final effort is aimed at opening up Apple's **Low Latency Wi-Fi Protocol**, which helps to decrease the lock-in of users into the Apple ecosystem by creating an open-source interoperable implementation of the protocol for Linux. This protocol underpins applications such as Continuity Camera (using an iPhone as external camera) and Sidecar (using an iPad as wireless additional display), meaning that if people want to switch away from the Apple ecosystem they will be able to do so in a gradual way – without immediate loss of functionality.

Projects involved in this cluster

Android translation layer (ATL): *Run Android apps on Linux*

VirtuAndroid: *Application-layer virtualization for Android apps*

SIMcurity: *Protect phones and users against SIM vulnerabilities and hostility*

Opening up Apple's Low Latency Wi-Fi Protocol: *Open-source interoperable implementation of LLW for Linux*

VoWiFi Watchdog: *Identify blocks and misconfigurations for VoWiFi*

The next cluster concerns **app stores**, again another one of the target areas identified for the programme. The app stores play a key role in the market dominance, acting both as gatekeeper and as a proprietary lever against OEMs – and they force the user to agree with terms and conditions they would probably not consent to given a real choice. The most important open source app store for Android (and part of the NGI Mobifree project) is F-Droid, and two project directly aim at improving that effort: **F-Droid App Overhaul** is modernising the F-Droid mobile app, while **LambdaNative F-Droid integration** is enabling developers using Scheme to directly publish to the F-Droid store.

Not all apps are free and open source, but users might still depend on some apps which don't comply with the strict policies of F-Droid – even if only for a transitional period. **IzzyOnDroid** is a popular third party repository for FOSS Android apps, built on top of F-Droid – facilitating users that need apps which don't fit into the main F-Droid store because of licensing or other requirements. **Termux** is another popular app distribution mechanism and runtime for Android, aimed at terminal apps. The project funded within Mobifree will allow external projects to use Termux execution environment in their own apps, and the project will also implement the new APK Library File (APKLF) execution/packaging design so that Termux can comply with security restrictions in Android 10 and newer that prevents apps from executing downloaded code. The project **Weblate Android SDK** will make it possible to decouple software distribution

and translation. Currently, adding or updating a translation requires a new release of apps. The SDK will empower users to update their translations immediately once a new translation/localisation for Android apps is available, which will speed up community translations and unburden the developers.

Projects involved in this cluster

IzzyOnDroid: *Third party repository for FOSS Android apps*

Termux: *Android terminal app and software distro/run-time*

F-Droid App Overhaul: *Modernise the F-Droid mobile app store*

LambdaNative F-Droid integration: *Portable, Productive and Performant App Development with Scheme*

Weblate Android SDK: *Live localisation updates for Android apps*

Users have come accustomed to proprietary tools and services which are useful and for which there are no good open alternatives available. **Maps** are one such domain, and as indicated above were specifically targeted up front as one of the topics of interest for Mobifree. **OpenAGPS** provides a privacy-friendly, self-hostable location service as a partial alternative to Google Maps, while **Easy Transit 2** delivers another part of the functionality of that app by building a public transit navigation app – even with some offline capabilities. An adjacent functionality is Google's Find Your Phone which locates your phone on a map; the project **Find My Device** replaces this service with a privacy-preserving alternative. Obviously, unlike the Google alternative this will also work in an emergency and disaster situation.

Google Translate is another widely used tool. **Offline Translator** and **RTranslator 3.0** are alternatives to Google Translate, but instead of leaking personal data to a remote service in another jurisdiction these projects providing the full translation on the user's device itself – and in the case of RTranslator even for spoken text. Again, because they are designed for offline usage these will work in emergency and disaster situations, for instance to communicate with people when international rescue teams enter a disaster area such as a flood or earthquake terrain.

Projects involved in this cluster

Offline Translator: *On-device translations using open models*

RTranslator 3.0: *Real-time local translation app for spoken word for Android*

FMD: *Privacy-preserving mobile device location*

OpenAGPS: *Privacy-friendly, self-hostable location service*

Easy Transit 2: *Public transit navigation app with some offline capabilities*

The remaining projects fall under ‘quality of life’ improvements for users and developers, ranging from input correction for a popular open source Android keyboard (**Unexpected Keyboard Autocomplete/Correct**) and more efficient text input for touch screen devices with **Gesture Typing** for AOSP-derived Keyboards. Users are very attached to specific input methods, but Google has all but abandoned the code in the original AOSP project. By supporting independent continuation of the development of these components, the entire Android ecosystem benefits.

Projects involved in this cluster

Unexpected Keyboard Autocomplete/Correct: *Input correction for popular alternative Android keyboard*

Gesture Typing for AOSP-derived Keyboards: *More efficient text input for mobile touch screen devices*

The two final projects are working towards the support for open standards, both within the World Wide Web Consortium (W3C). **Solid Share** develops a digital mobile wallet for W3C Solid, the standard for self-hosted LinkedData. and **CanIWebView** is aimed at standardisation of the so called **WebView**. One of the consortium partners within NGI Mobifree is the messaging app **DeltaChat**, which is the driving force behind a new app ecosystem built on web technologies called **WebXDC** which would benefit greatly from having a consistent and fully standardised WebView.

Projects involved in this cluster

Solid Share: *Digital Mobile Wallet for W3C Solid*

CanIWebView: *Contributing to standardisation of WebView in W3C*

Annexe

Overview of subgrantees

Androguard

Static and dynamic analysis of Android apps

Description

The Androguard project is used to analyze Android applications. This project marks a major evolution for Androguard, focusing on modernizing its architecture. The core strategy is to replace its monolithic structure with a suite of independent, native Python libraries for parsing essential Android files like AXML, APK, and DEX. This modular approach will make the tools easier to maintain, reduce external dependencies, and allow for greater flexibility.

Performance is a key driver of this initiative. To tackle the primary analysis bottleneck, a new high-speed dex-bytecode library will be developed in Rust with Python bindings. The main Androguard project will then be refactored to integrate these new, faster components, resulting in a cleaner and more efficient core tool for static analysis.

Building on this new foundation, the project will expand into advanced security domains. This includes APKXploit, a new tool for penetration testing; AndroidIR, which will enable sophisticated code analysis via an Intermediate Representation; and Androguard-MCP, an innovative plugin to help security engineers in discovering vulnerabilities more effectively.

BinaryAnalysis LLM Security

More info: https://nlnet.nl/project/Androguard

NGI MOBIFREE

APKpatcher/PyAxml

Support tool to manipulate APK and AXML file

Description

The Apkpatcher and pyaxml tools suite is used to analyze, unpack and pack APKs (the Android file format for applications) and also AXML and ARSC files used inside these packages to store data and metadata.

The core strategy is to be able to have a simple and modular way to manipulate these three formats for security reasons: to audit parsers, to audit applications (thanks to some features added to sniff the traffic or automatize some test directly by injecting code inside the APK) or to remove some trackers from an APK for privacy reasons. A code sharing website is planned, so users can share patches to remove trackers and keep control over their devices.

Analysis | Android | Mobile

More info: https://nlnet.nl/project/APKpatcher-PyAxml

Website: apkpatcher.ci-yow.com
Repository: gitlab.com/MadSquirrels/mobile/apkpatcher

Android translation layer (ATL)

Run Android apps on Linux

Description

The Android Translation Layer is an alternative implementation of Android application APIs on top of standard Desktop Linux, with the ability to run apps as-is using some AOSP components such as ART+libcore, modified to use system-provided libraries where possible to further the goal of being as lightweight as possible. That is in contrast with existing container-based solutions which require running a whole AOSP system in parallel to the host Linux system, resulting in considerably higher resource usage (both disk space and RAM) and longer startup times. The higher efficiency of ATL can make it viable to sideload apps also on more constrained devices. Another benefit of our approach is better integration with the desktop, such as native notifications.

Android | Emulation | MobileOS

More info: **https://nlnet.nl/project/ATL**

Website: gitlab.com/android_translation_layer/android_translation_layer
Documentation: gitlab.com/android_translation_layer/android_translation_layer/-/tree/master/doc

NGI MOBIFREE

Bugbane

App for self-conducting device forensics on Android devices

Description

Bugbane is a lightweight Android forensics and anomaly-detection tool designed to help users identify signs of compromise, including spyware, stalkerware, and other suspicious behavior, directly on their own devices. Bugbane builds on de-facto standard efforts such as MVT, reusing its indicators-of-compromise (IoC) formats and datasets, and is compatible with AndroidQF exports. It is designed to integrate easily into the existing workflows of civil society organizations, supporting their encryption tools of choice.

Bugbane operates on-device, without requiring additional hardware or rooting and guides users through a structured, user-friendly acquisition and analysis process. By simplifying data collection and consensual sharing of forensic artifacts with partner organizations, Bugbane aims to reach users who are typically outside established support networks, contributing to a broader and more accurate understanding of threats targeting civil society.

Android | Cybersecurity | Forensics

More info: https://nlnet.nl/project/Bugbane

Website: github.com/osservatorionessuno/bugbane
Fediverse: mastodon.cisti.org/@0n_odv

F-Droid App Overhaul

Modernise the F-Droid mobile app store

Description

F-Droid is a software ecosystem around Android applications. It is an app store kit, a platform, an app and catalogue of free and open source applications. The app makes it easy to browse and install apps, and redistribute these from your own device to others.

This project is about modernizing and rewriting the official F-Droid app that still dates back to the early days of Android in 2009. The goal is to make the app easier to use and more appealing especially for new users.

The rewrite will use the latest technologies and will make it easier and more attractive to contribute to the app while also making it easier for the maintainers to review and merge external contributions due to better test coverage and less code entanglement.

Appstore

More info: https://nlnet.nl/project/F-Droid-App

Website: f-droid.org
Repository: gitlab.com/fdroid/fdroidclient
Forum: forum.f-droid.org
Documentation: f-droid.org/en/docs

LambdaNative F-Droid integration

Portable, Productive and Performant App Development with Scheme

Description

LambdaNative is an free and open source framework that allows for creation of cross-platform applications, in particular on Android and general desktop operating systems such as Linux, BSD's, OS X or Windows. With LambdaNative, even someone with minimal programming background can create nice applications ranging from basic to advanced, using the Scheme programming language. This makes it very suitable for those that do not have a computer science background but still need to create a custom app - such as most researchers, educators and people working in the public sector.

The aim of the project is to add a LambdaNative pipeline to publish apps on the free and open source F-Droid app store. The second part of the project will create educational materials to teach people how to work with LambdaNative mobile application and how to publish their app.

Android DesktopApp Scheme

More info: https://nlnet.nl/project/F-Droid-LambdaNative

Website: www.lambdanative.org

FMD

Privacy-preserving mobile device location

Description

FMD allows you to locate and remotely control your Android device. This is useful if you have lost or misplaced it. FMD is decentralised, and users remain in full control of their data.

With FMD, you can send commands to your phone: to locate it via GPS, to locate it via nearby cell towers, to take a picture, to lock it, to let it ring, or to factory-reset it. Commands can be sent over multiple transport channels: over SMS, over third-party messaging apps like Signal or Matrix (that post a notification to the Android notification tray), or over the " FMD Server" (a self-hostable server providing a web interface to control your device).

Geo-localisation | RemoteControl

More info: **https://nlnet.nl/project/FMD**

Website: fmd-foss.org
Repository: gitlab.com/fmd-foss
Matrix: matrix.to/#/#fmd:matrix.org

NGI MOBIFREE

Gesture Typing for AOSP-derived Keyboards

More efficient text input for mobile touch screen devices

Description

HeliBoard is a very customizable and privacy-conscious open-source keyboard for Android. The current gesture typing feature, which lets you input words by swiping your finger over the letters, is only accessible when adding abandoned closed source code by Google.

Goal of this project is a well working and completely open-source implementation of gesture typing. Gesture typing quality will be ensured by sample contribution by developers and volunteers and comparison with results of said closed source code. The gesture typing library will be developed separately from HeliBoard, with a compatibility layer allowing it to be used as a drop-in replacement for said closed source gesture typing code. This approach will allow for compatibility with other virtual keyboards, mainly for Android, but also for other systems e.g. Linux.

Android Keyboard

More info: https://nlnet.nl/project/GestureTyping

IsMyPhonePwned

Scan phone security directly from a web browser

Description

" IsMyPhonePwned" is a new open-source initiative designed to put the power of security back into the users hands. By leveraging the speed and safety of Rust, the project allows anyone to run a comprehensive security scan on their phone directly from a web browser implementing WebUSB. There's nothing to install and no complicated setup; just a simple, clear process to check for compromise with complete anonymity and privacy.

" IsMyPhonePwned" aims to be more than just a tool; it's a statement that privacy is a fundamental right. By providing a free, accessible, and trustworthy way for journalists, activists, and any concerned citizen to secure their devices, we are building a community-driven defense against digital intrusion, one phone at a time.

Android Security WebApplication

More info: **https://nlnet.nl/project/IsMyPhonePwned**

Website: ismyphonepwned.com
Repository: github.com/IsMyPhonePwned

IzzyOnDroid

Third party repository for FOSS Android apps

Description

IzzyOnDroid provides Android apps which are available under free and open source licenses approved by OSI/FSF. With its more than 1,200 apps, this already popular repository is the largest third-party F-Droid-compatible repository - with more than 200,000 daily visitors on the primary site alone, not counting mirrors. Its intent is to provide useful apps, connecting a vibrant community of developers and users, with a focus on transparency, privacy, and security.

The goal of this project is to provide additional security, transparency, flexibility, and decentralization – e.g. by advancing our reproducible builds (which already cover more than a third of all apps in our collection) and making our tooling easier available for others to use.

Appstore MobileApp

More info: https://nlnet.nl/project/IzzyOnDroid

Website: izzyondroid.org
Repository: codeberg.org/IzzyOnDroid
Fediverse: floss.social/@IzzyOnDroid
Documentation: izzyondroid.org/docs

Opening up Apple's Low Latency Wi-Fi Protocol

Open-source interoperable implementation of LLW for Linux

Description

Apple developed a proprietary protocol called Low Latency Wi-Fi (LLW) that enables several inter-device streaming features in the Apple ecosystem. This link-layer protocol acts as the basis for applications with low-latency and real-time constraints, such as using a phone's camera wirelessly as a webcam on a laptop. This project focuses on implementing an open-source counterpart for Apple's LLW protocol stack on Linux, thereby providing interoperability of Apple platforms and bringing a useful low-latency protocol to the open-source community. This way, LLW will be available to third parties, which is of importance to strengthen end-users in having more choices and hindering Apple from gatekeeping technologies.

Linux | LowLatency | ReverseEngineering | Wifi

More info: https://nlnet.nl/project/LowLatency-Wi-Fi

Offline Translator

On-device translations using open models

Description

Offline translator is a privacy-focused application that handles multilingual needs entirely on-device, without sending data to external servers. It supports text and image translation with automatic language detection, transliteration across scripts, dictionary look-ups and text-to-speech functionality.

The app uses exclusively open code, models and datasets, and will contribute to those ecosystems as necessary.

MachineLearning Translation

More info: https://nlnet.nl/project/OfflineTranslator

OpenAGPS

Privacy-friendly, self-hostable location service

Description

Location-specific services benefit greatly from location awareness. However, satellite signals are slow and not always reliably available in urban areas (let alone inside buildings). Hence the need for " assisted GPS" , which uses alternate sources such as information based on mobile cell ids to determine location. While it seems obvious for such a capability to be a digital commons, there are no open services reliably providing this information- Mozilla operated something called the Mozilla Location Service, but this was retired recently. This leaves users either unserved or with a huge dependency on a few large vendors that bundle their own location service (based on non-public data sources and dark code) - with the latter users being dependent on the availability of and connectivity to specific machines on the internet. This project aims to provide a self-hostable alternative based on free and public sources, such as Galmon and OpenCellID, which would function independently from the services mentioned earlier.

GPS LocationBasedServices

More info: https://nlnet.nl/project/OpenAGPS

Website: openagps.net
Repository: gitlab.com/openagps
Documentation: gitlab.com/openagps/documentation

OWASP blint

Versatile binary linter, malware research tool and SBOM generator

Description

OWASP blint is an open-source binary linter and SBOM generator. The project had a humble origin as a linting tool, but soon found rapid adoption for a range of use cases such as malware identification (MalwareBazaar is a large-scale user), binary risk audits, and more recently binary SBOM generation for Android apk, go, dotnet, and rust binaries. The current version of Blint can already generate a granular SBOM for Android apk/aab files, up to some extent even from binary.

Within the scope of this grant, the team will enhance blint to improve package identification for native binary blobs (c/rust/kotlin native) bundled within an android app, will add fuctionality to identify cloud services, domain names, IP addresses, and other sensitive literals by performing static analysis on binaries. In addition support will be added for generating precise SBOM for swift binaries (unencrypted/debug files) by integrating blint with an LLVM frontend and a number of general improvements will be made to linting rules for mobile apps.

Linting SBOM Tracking

More info: https://nlnet.nl/project/OWASP-blint

Website: github.com/owasp-dep-scan/blint

PiRogue Tool Suite

Consensual mobile device forensic analysis and incident response solution

Description

The PiRogue Tool Suite (PTS) is an open source, consensual digital forensic analysis and incident response solution that empowers organizations with comprehensive tools for network traffic analysis, mobile forensics, knowledge management, and artifact handling. The tool suite includes both hardware and software components, with the PiRogue network router and Colander, a case management platform.

PTS aims to be a universally accessible and cost-effective solution for digital investigations, which is comprehensive, user-friendly design and modular. This allows for instance academics, civil society, and independent media to analyze artifacts, build investigations, and generate reports and intelligence feeds. This project will add support for dynamic analysis from emulated Android devices in addition to physical devices. implement TLS decryption for Flutter-based applications

Forensics | Mobile | TrafficAnalysis

More info: https://nlnet.nl/project/PiRogue-toolsuite

Pithus

Free and open-source mobile threat intelligence

Description

Pithus is a free and open-source Android threat intelligence platform aimed at activists, journalists, NGOs and researchers. Its goals is to provide intelligible and relevant information aggregated from several android application analysis tools to facilitate the understanding, reverse engineering, and threat analysis of android applications. Pithus adapts to its users by providing easy to read information on application behaviors, as well as precise technical data and analysis tools to detect similar malicious samples. Functionalities to easily pivot to other malwares of a same family, create custom detection rules, and monitor, detect and analyse new emerging threats. Pithus is community driven with an ever growing database of android applications.

This grant focuses on developing a number of new features and performing well overdue maintenance and necessary refactoring tasks, as well as provide adequate documentation and QoL improvements.

Mobile | MobileApps | ThreatAnalysis

More info: https://nlnet.nl/project/Pithus

Website: beta.pithus.org

SIMcurity: Tools for Securing the SIM interface

Protect phones and users against SIM vulnerabilities and hostility

Description

The SIMcurity project will develop new software and hardware tools to secure mobile devices against attacks from hostile SIMs. Often considered as root-of-trust in mobile communication networks, SIMs and eSIMs authenticate users and their equipment, including smartphones, cars, smart devices, and even trains. However, SIMs cannot always be trustworthy: rogue operators can update them remotely over the air, their communication interface is susceptible to machine-in-the-middle attacks, and the software running on them may itself have vulnerabilities. SIMcurity will shine light on this often overlooked attack surface, provide tooling to find and mitigate security flaws, and create strong defenses to protect users and their mobile communication.

SIM

More info: https://nlnet.nl/project/SIMcurity

Solid Share

Digital Mobile Wallet for W3C Solid

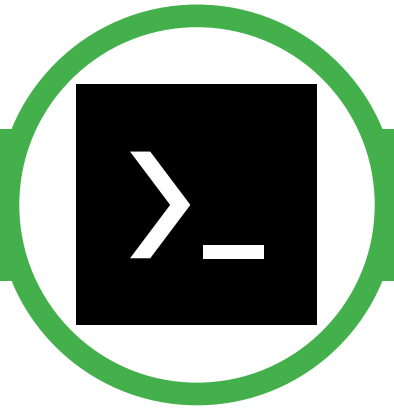
Description

This project works on a native app for the Android operating system, allowing citizens to use their solid pod as data and digital wallet. It allows users to login into their Solid pod with different accounts, manage their data (for instance also travel ticket and passes), share private files by means of a QR code, s and sync other Solid data modules (such as Contacts) within the Android ecosystem without needing extra apps. The app is designed offline-first. The goal of this project is to bring Solid into the hands of regular people, making them aware of the existence of the Solid project and allowing them to have a smooth and easy experience. It should be a base platform for using Solid pods as a daily usage storage as well.

Android MobileApp Solid

More info: https://nlnet.nl/project/SolidAndroidWallet

Repository: github.com/erfangholami/SolidShare



Termux

Android terminal app and software distro/run-time

Description

Termux is an Android app that provides a terminal emulator and a GNU/Linux distribution environment with 2000+ packages and executes programs natively on Android host OS/kernel, without any emulation or containerisation. It allows users to locally do most things that can be done on a Linux PC, like program in many languages, use text editors/IDEs, backup files, host websites and servers, and even run a full linux desktop interface. A termux-core library will be created which allows external projects to use Termux execution environment in their own apps. A new APK Library File (APKLF) execution/packaging design will be implemented so that Termux can comply with security restrictions in Android 10 and newer that prevents apps from executing downloaded code. Currently Termux works by being compiled in backward compatibility mode. Package sources will be patched to read paths from environment variables exported by the app, or compiled package files will be patched at install time, rather than relying on hardcoded paths in the package files to Termux rootfs.

Android | DeveloperTool | GUI | MobileApp | PackageManagement | TUI

More info: **https://nlnet.nl/project/Termux**

Website: termux.dev
Repository: github.com/termux/termux-app
Fediverse: fosstodon.org/@termux
Matrix: matrix.to/#/#termux_termux:gitter.im
Documentation: termux.dev/en/docs

Unexpected Keyboard Autocomplete/Correct

Input correction for popular alternative Android keyboard

Description

Unexpected Keyboard is a lightweight and privacy-conscious virtual keyboard for Android-based mobile operating systems. Its distinguishing feature is that you can type different characters by swiping your finger towards the corner of the key, a feature was originally designed for programmers using Termux. This allows to fit much more characters on screen than a regular keyboard layout, and prevents users from having to continuously switch just to input content containing characters spread across layouts. This project will add (offline) word suggestion and correction to Unexpected Keyboard, which well help to make the app even more user-friendly.

Android InputDevice Keyboard

More info: https://nlnet.nl/project/UnexpectedKeyboard

Website: github.com/Julow/Unexpected-Keyboard
Repository: github.com/Julow/Unexpected-Keyboard

VoWiFi Watchdog

Identify blocks and misconfigurations for VoWiFi

Description

VoWiFi (Voice over WiFi, also WiFi-calling) is the preferred channel for voice calls and messages for 4G/5G for most operators and operating systems (i.e., Android, iOS). However, there is a lack of transparency regarding existing operator practices and the security of everyday voice calls and messages. There are shocking security weaknesses such as default and static private keys, insecure configurations, as well as anti-consumer practices (geoblocking) at live operators.

Operators still use shared private keys to encrypt their customers' communication, allowing adversaries to eavesdrop on calls and messages. Due to the lack of transparency, customers have no way of evaluating the settings for their current operator and operators have little incentive for improvements. The VoWiFi Watchdog project will regularly probe operator's VoWiFi configurations to detect deployed geoblocking measures and expose deprecated security settings. The scan results will be automatically published at our project platform, allowing customers to check their current (or future) operator, motivating operators to upgrade insecure setups. This will help to bring transparency to the VoWiFi ecosystem.

Netneutrality | VoWiFi | Voicecalling

More info: https://nlnet.nl/project/VoWiFi-watchdog

CanIWebView

Contributing to standardisation of WebView in W3C

Description

Web technologies like HTML, CSS and JavaScript are also used very much outside of a Web browser, because they are well standardized, openly available and many developers know how to build for the web. WebViews are software components used to render Web content inside native apps. They are integral to the mobile web experience, as in-app web content display for social media and serving as a foundation for entire applications and games built with web technologies. WebViews are, however, very much overlooked by web developers, web standards developers, and browser engine vendors in terms of compatibility and feature availability.

As part of the W3C WebView Community Group, this project addresses a critical gap in the web platform by establishing comprehensive testing infrastructure and resources for WebView compatibility. The initiative will deliver three key components: open-source testing applications for Android and iOS distributed through app stores, automated testing infrastructure using WebDriver-like tools for continuous compatibility monitoring, and the caniwebview.com website as resource for WebView compatibility data and documentation. Through regular meetings and conference sessions with stakeholders in the WebView space this project aims to improve the user experience, address common issues and lay foundations to future standards.

Compatibility | Standardisation | Webview

More info: https://nlnet.nl/project/W3CWebview-tooling

Coda

Each of the efforts included in this bookled contributes to a **more trustworthy**, **resilient** and **sustainably open** internet in its own unique way. By helping redecentralise the internet, they are bringing a better internet a step (or even a few steps) closer. We salute all those people working towards an internet for all, also in the wider free and open source community.

Finally, our sincere gratitude to the members of the external review committee that kept a close watch on the eligibility of the projects. You all made a difference.

MOBIFREE

Colofon

NGI Mobifree is made possible with financial support from the European Commission's **Next Generation Internet** programme, under the aegis of **DG Communications Networks, Content and Technology**.

NGI Mobifree is a collaboration between the following partners:

— E Foundation
— Waag Futurelab
— Murena
— QWANT
— Rapid.Space International SAS
— Merlinux GmbH
— Lars Marvin Wißfeld
— Daniel Gultsch
— Stichting Art — Technology
— NLnet Foundation
— University of Amsterdam
— Evidence Aid
— Uptodown Technolgies SL
— Code for Romania
— Biosense Institute

Designed and typeset in the Netherlands in Source Sans Pro with free & open source software only: Inkscape, Typst and Vim. Hex logo's can be downloaded via: https://nlnet.nl/hex

---

Project officer:

— Ragnar Bergström

Financial officer:

— Stéphane Andries

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101135795.

NGI ZERO