

Libertaria:progetto Titania

WhitePaper

19/11/17

Version1.0



T I T A N I A

collaboratori:

Markus Maiwald, Oleksiy Protas, Pooja Maheshwari,
Sarah Klostermair

Disclaimer

Questo documento è un documento vivo. Come tale, sarà rivisto per soddisfare le esigenze di un futuro che non sempre possiamo prevedere. I lettori interessati a maggiori informazioni su Titania, sulla sua collocazione in libertaria e sulla sua relazione con altri progetti di libertaria facciano riferimento alla sezione di lettura successiva alla fine di questo documento.

Introduzione

La recente ondata di interesse per la decentralizzazione e le sue tecnologie associate è stata accompagnata da un focus rinnovato sul modo in cui la decentralizzazione può ostacolare i nostri attuali sistemi sociali, politici ed economici e portare più equità e libertà ai miliardi di persone che sono trascurate dall'attuale status quo, fornendo un accesso più universale alla tecnologia e alle opportunità e eliminando intermediari indesiderati. Benché la promessa della decentralizzazione sia reale, pochissimi progetti la stanno mantenendo bene .

Il problema principale è la mancanza di considerazione delle esigenze e dell'esperienza degli utenti. Se la tecnologia di decentralizzazione andrà a beneficio delle persone che realmente ne hanno bisogno, deve essere ottimizzata per soddisfare le loro esigenze, capacità e livello di risorse.

Molto è stato realizzato con la proliferazione della tecnologia di comunicazione attraverso il mondo sviluppato -uno studio molto citato ha stimato che 6 miliardi persone hanno accesso ai telefoni cellulari contro solo 4,5 miliardi hanno che accesso a un WC nel posto di lavoro.¹ Ma non si considera che molti di questi dispositivi sono vecchi, parzialmente funzionali e gli utenti hanno competenze tecniche molto limitate.

Le nuove tecnologie sono anche dotate di barriere ad alta capacità. Con il tempo queste tecnologie diventano abbastanza semplici da utilizzare e capire per la maggior parte delle persone, di solito vengono cooptate da aziende o governi e drenati della maggior parte del loro potenziale.

TitaniaOS è un sistema operativo basato su Linux che è ottimizzato per funzionare su quasi tutti i dispositivi smartphone o Internet - ready, trasformandoli rapidamente e semplicemente in un nodo completo o parziale nella rete decentralizzata peer-to-peer di libertaria.

Grazie alla sua interfaccia intuitiva, gli utenti saranno in grado di utilizzare TitaniaOS per eseguire rapidamente e facilmente una varietà di compiti, tra cui la configurazione e la personalizzazione del loro nodo, la navigazione e l'installazione di dApps e anche la creazione di una propria blockchain personalizzata usando il protocollo Hydra di libertaria.

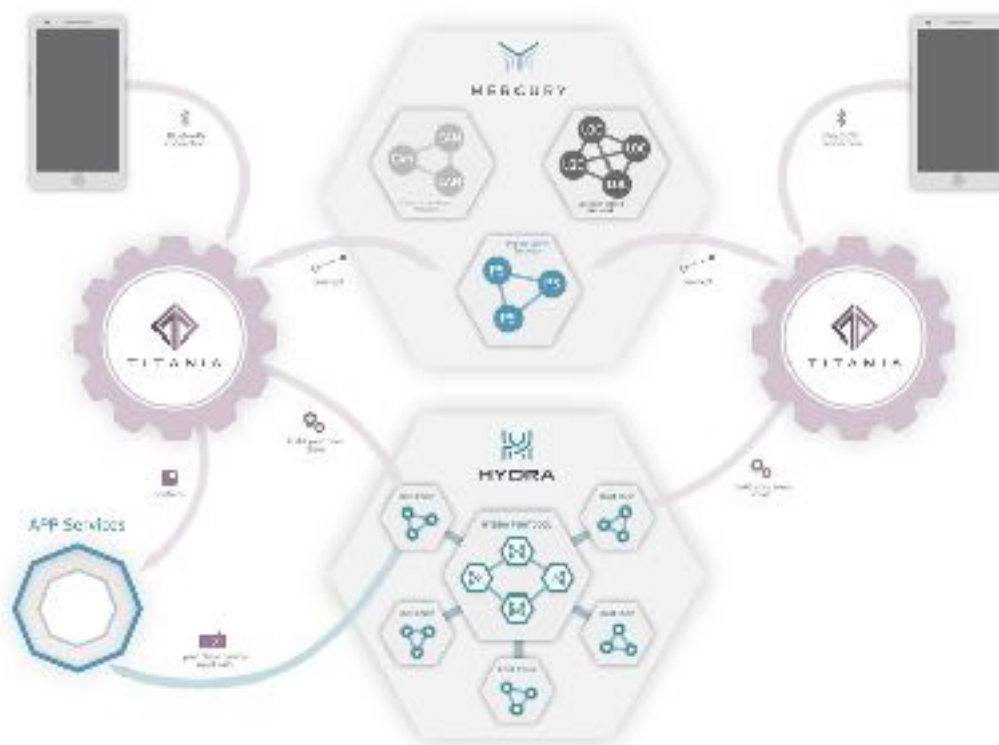
Fornendo queste funzionalità e avendolo disegnato avendo in mente tutti, Titania darà vita alla promessa di decentralizzazione, fornendo libertà e opportunità a coloro che più ne hanno bisogno.

1 <http://www.un.org/apps/news/story.asp?NewsID=44452&Cr=sanitation&Cr1=#.WgtgwmhSzIX>

TitaniaOS

Panoramica

Un protocollo peer-to-peer (P2P) come Mercury è utile solo se ci sono “equivalenti” sufficienti per far funzionare la rete. Tuttavia, la maggior parte delle persone non hanno la competenza o le risorse per aderire a tale rete. Titania è progettato per affrontare questo problema e formare la spina dorsale dell'ecosistema decentralizzato di libertaria.



TitaniaOS è un sistema operativo Linux Embedded personalizzato progettato per essere installato su vari dispositivi, tra cui smartphone, vecchi dispositivi ed elettrodomestici. TitaniaOS è ottimizzato per eseguire il protocollo Mercury, e rendere facile per chiunque avere il proprio nodo di rete a casa senza necessità di un PC acceso tutto il giorno o con una configurazione iniziale tecnicamente impegnativa, anche se naturalmente gli utenti saranno in grado di personalizzare completamente i propri dispositivi.

Con TitaniaOS, i nodi saranno distribuiti in modo sicuro per la nostra rete P2P libertaria in maniera molto semplice e conveniente. L'utente ha il pieno controllo sul proprio nodo e può connettersi ad esso tramite il proprio smartphone.

Con le applicazioni scaricabili, TitaniaOS può anche diventare contemporaneamente un router wireless, una TV o un hub di casa intelligente, cosicché gli utenti possano dare alle loro attrezzature un uso ibrido. Le versioni Embedded di TitaniaOS sono abbastanza leggere e portatili per poter funzionare su telefoni cellulari vecchi o rotti, fornendo seconda vita all'elettronica e riducendo i rifiuti.

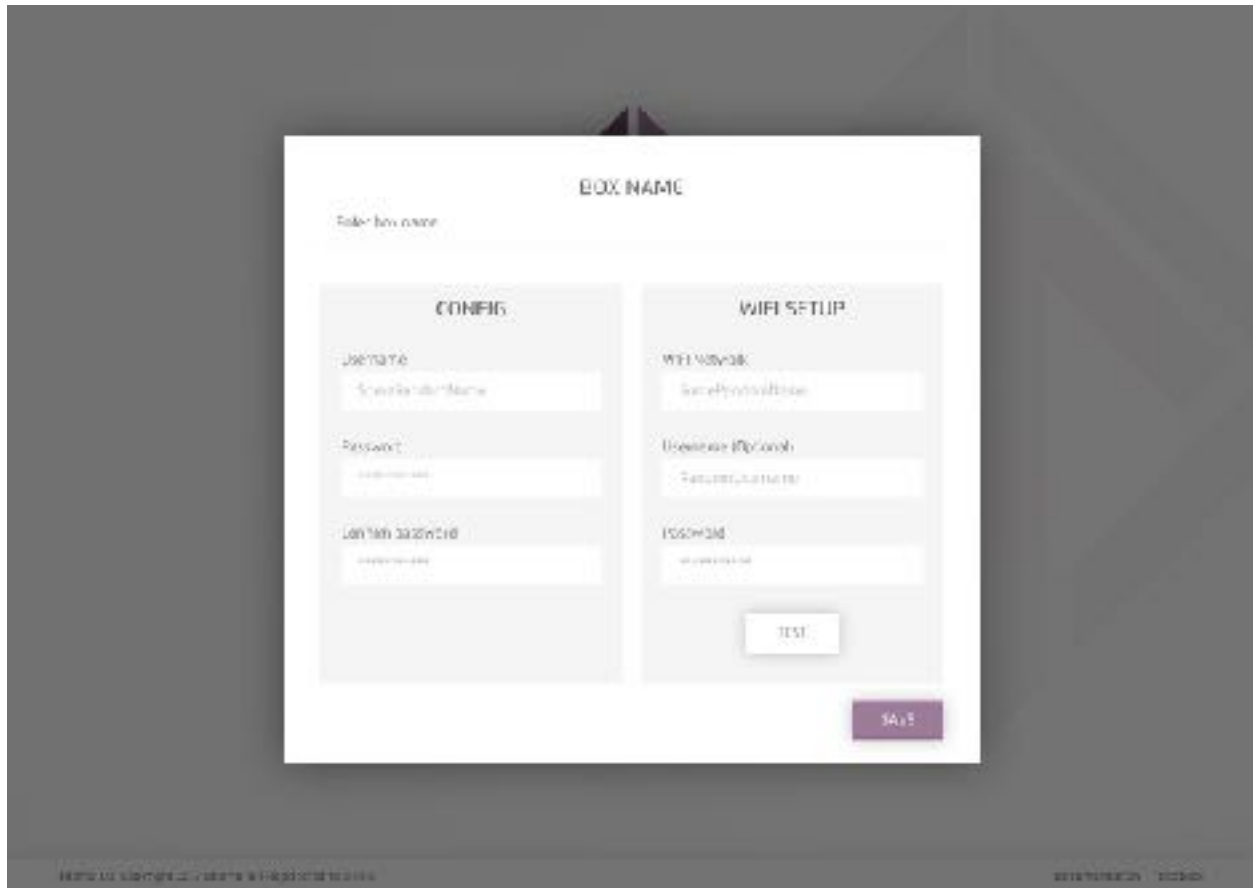
Struttura

Titania è una distribuzione Linux basata sui progetti OpenEmbedded e Yocto. La maggior parte delle funzionalità finali dell'utente viene implementata in contenitori separati per ragioni di sicurezza e il livello più esterno del sistema contiene solo il software più critico. Il sistema principale consiste principalmente nel sistema di inizializzazione del sistema, il NetworkManager per fornire connettività, un servizio personalizzato di monitoraggio backend e il daemon Docker che consente il supporto dApp. Per impedire il blocco del sistema, Titania fa uso di un meccanismo chiamato watchdog, che lo induce a riavviare automaticamente ogni volta che il software di sistema non riesce a notificare l'hardware in tempo. Il sistema viene eseguito in sola lettura per impedire al malware di infettare i programmi e tutti i file modificabili vengono fatti per essere spartiti in una partizione separata che rende più facile il recupero degli incidenti. Ancora un'altra partizione viene utilizzata come spazio di archiviazione per dApps e per i contenitori di sistema, sia per il software sia per i dati.



Interfaccia

TitaniaOS sfoggia una chiara, elegante interfaccia grafica utente (GUI), che chiunque può capire e utilizzare. La prima volta gli utenti vengono configurati con un semplice insieme di domande, per determinare le loro esigenze e le abitudini di utilizzo previste e di conseguenza personalizzare la loro esperienza. Una volta collegato alla rete libertaria, navigando nel dApp Store le dApps saranno familiari agli utenti di servizi simili su piattaforme centralizzate.



TitaniaOS è completamente modificabile e riconfigurabile. Gli utenti più esperti possono accedere a queste e altre funzionalità tramite un'interfaccia a riga di comando.

Sicurezza

La sfida

Titania inevitabilmente attirerà l'attenzione degli hacker. Quindi, la sicurezza è fondamentale. Come per ogni grande impresa tecnologica, ci sono due approcci principali alla sicurezza: prevenzione e mitigazione.

Ovviamente, dobbiamo garantire che la nostra sicurezza sia il più robusta possibile, individuando potenziali debolezze e vettori di attacco e mettendo in atto misure per bloccarle. Ma è ingenuo supporre che questo sarà un completo successo. Nessun software o hardware è mai completamente sicuro. Pertanto, è anche importante progettare la sicurezza con mitigazione in mente: nelle rare ma inevitabili occasioni che gli hacker siano in grado di trovare un exploit, il sistema dovrebbe minimizzare i danni che possono fare.

Questa è la strategia di sicurezza migliore per qualsiasi progetto. Tuttavia, le ramificazioni tecnologiche ed etiche della decentralizzazione aggiungono maggiore complessità. Titania è la porta d'accesso per la rete libertaria più ampia e le sue dApps. Libertaria è concepito come un sistema davvero decentralizzato, quindi non possiamo e non dovremmo imporre il controllo su chi si unisce alla rete e su quale software è costruito dagli utenti ed è disponibile per loro. Ciò significa che la mitigazione assume un ruolo ancora più forte del solito nella sicurezza per Titania.

Infine, libertaria è progettata per tutti, indipendentemente dal loro livello di competenza. Mentre la sicurezza è fondamentale, abbiamo anche cercato di garantire che questa sicurezza non rendesse Titania ingombrante o fuori luogo per gli utenti a cui è destinato. Dove possibile, le caratteristiche di sicurezza inintrusive e semplici.

Le seguenti sezioni spiegano i tre principali problemi di sicurezza che abbiamo individuato e le soluzioni che abbiamo adottato per TitaniaOS.

Problemi

Sicurezza dApp

Il dApp Store Libertaria sarà completamente decentralizzato e gratuito. Non ci può essere censura di accesso o di contenuto. Ma è ingenuo supporre che tutti rispettino queste libertà. Questo sistema non solo dà libertà agli utenti malintenzionati, li attrae. Pertanto, dobbiamo fare tutto il possibile per proteggere la stragrande maggioranza degli utenti ben avvisati e degli sviluppatori, rispettando i principi di libertà e decentralizzazione.

Errori umani

I problemi di sicurezza non si limitano agli hacker. Molti problemi sono causati da codici scadenti o incompleti. Ci aspettiamo utenti e sviluppatori di ogni genere di livello di abilità e abbiamo bisogno di essere preparati per tutti i problemi che porteranno.

aggiornamenti

La natura decentralizzata di Titania e l'intricata configurazione introducono una certa complessità di manutenzione. TitaniaOS dovrà essere aggiornato di volta in volta, ma senza server centrale da cui far partire l'aggiornamento a tutti i nodi, la rete stessa dovrà essere in grado di aggiornarsi. Questo è reso più difficile dalla natura di questi nodi: ci aspettiamo un sacco di dispositivi di fascia bassa con la connettività degli utenti da posizioni con connettività intermittente.

Dobbiamo aspettarci che gli utenti aggiornino di rado, e che molte versioni differenti di TitaniaOS siano attive contemporaneamente sulla rete.

Dal momento che non possiamo e non dobbiamo impedire agli utenti di aderire alla rete, dobbiamo anche diffidare di nodi maligni o dei nodi falsi.

L'aggiornamento decentralizzato è anche molto meno affidabile rispetto al suo equivalente centralizzato, quindi ci deve essere anche un sistema di backup attivo, per quando le cose vanno male.

Soluzioni

Sicurezza dApp

Nel peggiore dei casi, dobbiamo garantire che una violazione della sicurezza non consenta agli intrusi di accedere alla rete più ampia. La soluzione standard sarebbe quella di eseguire ogni applicazione in un ambiente virtualizzato. Tuttavia, questo richiede un potente hardware del server e Titania è progettato per girare su dispositivi di fascia bassa. Risolviamo questo problema utilizzando la tecnologia di contenimento con Docker/LXC, che fa girare ogni applicazione in un ambiente isolato. L'utilizzo di Docker consente inoltre di riutilizzare i blocchi dei contenitori, il che si traduce in un enorme risparmio di spazio su disco, memoria e tempo di sviluppo.

Errori umani

Forniamo inoltre un SDK di App basato su Rust, per impedire le violazioni basate sull'errore umano. Tutti i componenti dell'SDK così come il sistema di base stesso sono costruiti con dei rinforzi preinseriti in modo che gli attacchi trovino molto più difficile sfruttare il livello di codice della libreria dell' app a loro vantaggio.

Aggiornamenti

Per mantenere l'operazione senza problemi per l'utente, Titania sfoggia un filesystem dual-root che può tornare a una versione stabile nel caso di un aggiornamento parziale o fallito. In linea con l'ecosistema distribuito che fornisce, Titania può raccogliere i suoi aggiornamenti da file System peer-to-peer come IPFS. Qui è anche dove le applicazioni sono pubblicate e scaricate. Non diversamente da BitTorrent, i nodi Titania partecipano alla diffusione degli aggiornamenti, il che elimina un punto centrale di fallimento e migliora la larghezza di banda complessiva dell'aggiornamento senza bisogno di una CDN vera e propria. Ogni aggiornamento viene firmato in modo crittografico per garantire che i nodi possano fidarsi del software che stanno installando.

Monitoraggio

Titania 1.0 è progettato per offrire ai suoi utenti un'installazione semplice ed a manutenzione zero per una sicura unità standalone che aiuterà gli utenti finali a formare comunità autosufficienti in base al proprio modello di fiducia.

Conterrà una semplice configurazione guidata e un dashboard. Il dashboard conterrà una panoramica di tutte le applicazioni installate sul dispositivo.

Il drill-down sul dashboard fornirà un resoconto dettagliato dell'integrità delle applicazioni in esecuzione sul dispositivo.

Titania verrà fornito con applicazioni pre-installate come il server di profilo e il server basato sulla posizione. Titania sarà ad auto-monitoraggio, con iterazioni per crash e segnalazione di anomalie da parte di nodi attendibili e un App Store nelle fasi successive.

Potrebbe non sembrare immediatamente utile avere un modello di monitoraggio nella prima interazione di uno strumento come Titania, ma funge anche da modulo di gestione degli attacchi

Al fine di ottimizzare lo spazio di archiviazione per il monitoraggio su dispositivi Titania, usiamo un modello quasi in tempo reale per il monitoraggio.

Le metriche come uptime, vengono raccolte in un tempo di risposta medio e in un utilizzo della memoria in un intervallo ricorrente.

Le metriche hanno un periodo di conservazione.

Non appena un'immissione passa un periodo di memorizzazione, il sistema di monitoraggio viene aggregato e memorizzato.

Tutti i dati prima del periodo di conservazione vengono conservati in forma aggregata. L'utilizzo di un modello come questo garantisce la scalabilità in caso i nodi decentralizzati formino sempre una gerarchia.

Il monitoraggio decentralizzato richiede molti compromessi, ad esempio la ridondanza dei dati raccolti, i principi di attendibilità e la creazione di report quando vengono superate le soglie.

La ridondanza dei dati si verifica non appena un nodo sceglie un altro nodo per monitorarlo.

Per ogni nodo che ha scelto si penserà che la loro è una connessione isolata e quindi si aumenterà la ridondanza.

Gli eventi altereranno il meccanismo il quale avviserà gli utenti se qualsiasi anomalia è prevista studiando i valori Delta dai dati di monitoraggio raccolti.

Poiché questo nodo è connesso ad altri nodi, qualsiasi trap o trasmissione generata verrà ripetutamente inviata allo stesso nodo disturbato.

Puntiamo a gestire questi avvisi in modo che colpiscano lo stesso endpoint nel nodo, per accertare che il nodo non sia bombardato con gli avvisi da tutti i nodi simultaneamente.



Gli utenti stessi possono decidere il loro modello per il monitoraggio, da semplice ad avanzato. Per esempio, un utente può scegliere di essere monitorato dal supporto Titania, o un cliente laico può decidere di essere guidato da un super-utente, che potrebbe fornire assistenza a fronte di un pagamento.

TitaniaBox

I box Titania sono una specifica implementazione di TitaniaOS progettata per la prima volta per gli utenti.

Un box Titania è un'unità di nodi standardizzata con TitaniaOS pre-installato.

L'obiettivo è quello di essere il più vicino possibile al progetto chiavi-in-mano: gli utenti possono semplicemente collegare la loro casella Titania ad un router tramite il cavo in dotazione e può essere accessibile e funzionante in pochi minuti.

L'interazione corrente del box Titania è un Raspberry Pi con TitaniaOS installato tramite lo slot per schede SD.

Tuttavia, in futuro l'obiettivo è quello di creare la nostra soluzione hardware su misura.

Ulteriori letture:

[Libertaria White Paper](#)

[Mercury White paper](#)

[Open Embedded project](#)

[Yocto Project](#)

