

NOX – نقشه راه

مقدمه

سیستم NOX برای ارتباط رایگان، پیام‌رسانی و تبادل داده بدون واسطه‌ها و سرورهای متمرکز طراحی شده است. این سیستم با اولویت حفظ حریم خصوصی و عدم جمع‌آوری اطلاعات توسعه یافته است. قابلیت‌ها در هر نقطه‌ای از جهان، بدون توجه به کشور، وضعیت اجتماعی یا موقعیت مکانی کاربر، در دسترس هستند.

تعاریف

– کاربر: فردی که در شبکه NOX مشارکت می‌کند بدون نیاز به ثبت‌نام اجباری یا ارائه اطلاعات شخصی.

– ارتباط مستقیم: تبادل داده‌ها بین دستگاه‌ها بدون دخالت شخص ثالث یا گره‌های متمرکز.

– رمزنگاری عمیق: اصطلاحی اختصاصی در سیستم NOX که به مجموعه‌ای از روش‌های رمزنگاری اطلاق می‌شود که نه تنها محتوای ارتباطات را محافظت می‌کنند، بلکه وجود خود ارتباط را نیز پنهان می‌سازند.

– نشست: بازه زمانی موقتی از تعامل که پس از پایان آن، داده‌ای ذخیره نمی‌شود.

اصول

– عدم ذخیره‌سازی داده‌ها: مکالمات، فایل‌ها و متادیتاها توسط سیستم ذخیره نمی‌شوند.

– استقلال: عملکرد بدون نیاز به ثبت‌نام و با امکان ناشناس ماندن کامل.

- پایداری ارتباط گروهی حتی در زمان قطع اتصال اینترنت.
- نامرئی بودن ارتباطات: ترافیک غیرقابل شناسایی، فیلتر یا ردیابی.
- روش‌های رمزنگاری به‌کار رفته پایه رمزنگاری عمیق را تشکیل می‌دهند.
- رایگان بودن: بدون محدودیت مالی یا نیاز به اشتراک.

اهداف

1. فراهم‌سازی ارتباطی ایمن و پایدار در هر شرایطی، حتی در شرایط بحرانی.
2. ایجاد زیرساختی مستقل و مقاوم در برابر سانسور و مسدودسازی.
3. تضمین ناشناس‌بودن و حفظ حریم خصوصی هر کاربر.
4. ارائه ابزارهای جهانی ارتباطی در سراسر جهان.
5. حفظ سادگی استفاده بدون نیاز به تجهیزات خاص.

مدل تهدید

- سانسور محلی و جهانی.
- جمع‌آوری و تحلیل هدفمند اطلاعات شخصی توسط سرویس‌های جهانی.
- تحلیل الگوهای تعامل برای ساخت نقشه ارتباطات و عادات کاربران.
- تلاش برای مسدودسازی کانال‌های ارتباطی.
- قطعی‌های محلی و جهانی اینترنت.

مراحل اجرا

مرحله ۱ – عملکرد پایه

– ارتباط مستقیم بین کاربران بدون شخص ثالث یا گره متمرکز، با پایداری برای ارتباطات گروهی هنگام قطع اینترنت.

– عملکرد کاملاً مستقل بدون نیاز به ثبت نام.

– دسترسی رایگان به قابلیت‌ها در هر نقطه‌ای از جهان.

– پشتیبانی از پیام‌رسانی، فایل، صدا و ویدئو.

– تماس صوتی P2P شبیه تماس تلفنی بدون سیم‌کارت یا شماره.

– تبادل کلید ایمن و آنی.

– مکانیزم رمزنگاری عمیق برای پنهان‌سازی ارتباط و محافظت در برابر رهگیری.

مرحله ۲ – گسترش قابلیت‌ها

– ایجاد و انحلال پویا برای گروه‌های امن بدون ذخیره‌سازی داده پس از نشست.

– معماری ماژولار برای اضافه/جایگزینی اجزا بدون توقف سیستم.

– ادغام کانال‌های چندپروتکلی برای افزایش قابلیت اطمینان.

– ابزارهای پیشرفته برای تبادل امن فایل و رسانه.

– کنفرانس‌های تصویری رمزگذاری شده.

مرحله ۳ – افزایش پایداری و سازگاری

– تقویت مقاومت در برابر تهدیدهای جدید فنی و سانسوری.

— به روزرسانی روش‌های رمزنگاری و مکانیزم رمزنگاری عمیق.

— اقدام پیش‌دستانه در مواجهه با ریسک‌های متغیر فنی و شبکه‌ای.

مرحله ۴ — اکوسیستم و یکپارچگی‌ها

— API برای ادغام NOX با اپلیکیشن‌ها و سرویس‌های دیگر.

— پشتیبانی از پرداخت‌های ناشناس و ریزتراکنش‌ها در شبکه.

— ادغام با کلیده‌های سخت‌افزاری و دستگاه‌های ایمن.

— (بدون ذخیره‌سازی داده‌ها: یکپارچگی‌ها اصل عدم حفظ محتوا و متادیتا را تغییر نمی‌دهند.)

مرحله ۵ — جامعه و خودگردانی

— ایجاد سیستم غیرمتمرکز برای مدیریت جمعی پروژه (DAO).

— مکانیزم‌های شفاف برای پیشنهادات و رأی‌گیری.

— برنامه‌های حمایتی برای توسعه‌دهندگان و پژوهشگران امنیت.

— آزمون‌های عمومی و یاداش برای شناسایی آسیب‌پذیری‌ها.

نتیجه‌گیری

ما به‌سوی سیستمی مستقل، مقاوم و در دسترس جهانی برای ارتباطات در حرکت هستیم که آزادی ارتباط را حتی در برابر فشار، مسدودسازی و رهگیری حفظ می‌کند. NOX فقط یک ابزار نیست، بلکه فضایی است که در آن هر فرد آزاد می‌ماند و تعاملات در برابر کسانی که می‌خواهند کنترل کنند، محافظت‌شده و نامرئی باقی می‌ماند.