Redesigning the Internet for the 21st Century

Our vision is to fundamentally redesign the way how data is routed, transmitted and handled on the Internet in order to provide private, confidential and censorship-resistant means of communication for billions of users.

This project, supported by the Wau Holland Foundation, was born out of our dissatisfaction with the technological status quo of the Internet. It is time to get rid of legacy technologies with fundamental design flaws that enable the widespread exploitation of sensitive data for purposes of mass surveillance, cyber crime and economic espionage.

We are an international, interdisciplinary group of experts with years of experience in fields such as distributed systems and cryptography. Together, we aim at realizing a new Internet architecture that enables informational self-determination and truly serves the needs of free and democratic societies.

Design Principles

Data security is at the core of our technical approach. It is not sufficient to only secure the contents of communications. We also want to prevent the systematic collection of commmunication profiles (metadata), as the analysis of the social graph of a population poses a particular threat to democracy.

Our concept for a new Internet is based on the following design principles:

- **ubiquitous end-to-end encryption**, removing the necessity to trust any third parties that might access our data while it is being transmitted or stored
- **obfuscation of transmission patterns**, preventing the analysis of social relations, behavior patterns and topical interests of the participants in a network
- **decentralized authentication mechanisms**, removing the necessity to trust centralized certification authorities that can be compromised
- **multicast technology,** because we need to interconnect billions of users without the need for centralized server farms
- **distributed data flow and storage**, making bulk collection of data economically unattractive
- **consistent use of free and open software**, putting the system under permanent public scrutiny and giving users control over their computation

Beyond the application of cutting-edge security standards, our concept emphasizes scalability and usability. We want to establish an attractive technological platform for applications and commercial services that can be used by large user bases worldwide.

Using a modular approach, we are integrating existing best practices and results from the scientific community to build a coherent system.

Development Plan

Our aim is to provide alternatives to unsafe technologies for all relevant modes of communication that are popular with Internet users today. Under the assumption that funding can be secured, we came up with the following roadmap, which is a scenario based on our current knowledge of activities.

Phase 1 (within 2 years)

Product description	**as an alternative to**
Secure business transactions by means of decentralized authentication for web services	TLS/SSL (HTTPS), X.509 (certification system)
Server-based confidential one-to-one and group telephony	Skype, Flash telephony, telephone, VoIP
Instant one-to-one and group messaging	Facebook chat, Whatsapp, IRC, XMPP/Jabber
Anonymized distributed data storage	Cloud based apps, unencrypted servers
Integration of anonymous browsing	Tor, I2P

Phase 2 (within 5 years)

Product description	**as an alternative to**
Asynchronous one-to-one messaging with attachments	Facebook mail, simple e-mail functions
Asynchronous mailing lists for group collaboration with distributed storage	advanced e-mail functions, Facebook groups, message boards, Dropbox
Distributed web, multimedia and streaming services	Websites, Podcasting, Youtube, Content Delivery Networks (CDN)
Distributed social networking platform	Facebook, Google Plus, Diaspora
Audio and video group communication	Google Hangouts, Skype conferencing, telephone and VoIP conferencing
Decentralized news distribution	Reddit, Google news
Anonymous, taxable payments	Visa, Paypal, Bitcoin

Phase 3 (long-term)

Product description	**as an alternative to**
Decentralized, censorship resistant search engine	Google search, Yahoo search, Microsoft Bing
Migration to public key based routing	BGP, OSPF
Free and open hardware	Proprietary processors and peripherals (Intel, AMD)

Supported by

wauland.de - youbroketheinternet@wauland.de

GNUnet.org

secushare.org