Bitmessage

Szenario: Die Gegenwart

NSA überwacht das gesamte Internet

CAs sind nicht vertrauenswürdig (DigiNotar)

Firmen geben NSA Serverzugriff

Wie sähe die passende Email-Alternative aus?

Bitmessage

File Settings Help

Inbox | Send | Sent | Your Identities | Subscriptions | Address Book | Blacklist | Network Status

Search

All

To	From	Subject	Received
onli	**bitmessage.ch gatew...**	**test des kompletten ...**	**Sa, 03 Aug 2013 01:44**
onli	**bitmessage.ch gatew...**	**test des mailservers**	**Fr, 02 Aug 2013 08:38**
onli	bitmessage.ch gateway	bitmessage.ch forward ...	Do, 01 Aug 2013 09:25
onli	bitmessage.ch gateway	test bitmessage.ch to bi...	Mo, 29 Jul 2013 11:29
onli	echo server	ECHO: test echo	Mo, 29 Jul 2013 11:26
onli 2	BM-omXeTjutKWmYgQJj...	ECHO: echo other server	Mo, 29 Jul 2013 09:59

1. Verschlüsselung als Standard
2. Größtmögliche Anonymitätsmenge
3. Kein zentraler Angriffspunkt

Trustless

Verschlüsselung als Standard

Automatisch: Gesendete Nachricht mit public Key des Empfängers verschlüsseln

Elliptic Curve Encryption => AES-256-CBC

Größtmögliche Anonymitätsmenge

Alle Nachrichten werden an alle Teilnehmer des Netzwerks geschickt -> Kein Privacy-Problem, da verschlüsselt

Skaliert das? Nein.

Kein zentraler Angriffspunkt

P2P-Netzwerk

Jeder Node gibt Adresse aller anderen

Alle haben alles

Wie funktioniert das Netzwerk? No fucking clue

Zeug

POW

Installation

FOSS

Streams

POW

Spambekämpfung durch Rechenzeitaufwand

Installation

Einfaches Python-Programm

FOSS

selbstverständlich: https://github.com/Bitmessage/PyBitmessage

Streams

Notbehelfsskalierung

A1, …, AN in Stream 1
B1, …, BN in Stream 2
….

Aufsplittung in Anonymitätsklassen

Danke

http://www.onli-blogging.de

BM-GuFG7jBPbuXVXTn9L9CvnD6zdNy3eTnV

Zusatz: Angriffe

Angriff 1: Phishing

Bitmessage has several potential security issues including a broken proof of work function and potential private key leaks.

Full details:

http://secupost.net/2325962497/bitmessage-security

Angriff 2: POW + Adressbuch

Kontakte im Adressbuch => POW = 1

Alice + Bob kennen sich

Alice erstellt geheime 2. Adresse.

Bob schreibt an diese. POW für ihn ist 1 -> Bob weiß, dass die geheime Adresse ihn im Adressbuch hat.

Zusatz: Mailsetup

Mit Mailclient BMs senden und empfangen

mailadresse ->

BM-....@bitmessage.ch ->

echte BM auf Heimserver mit POP-enabled BM-Client[1] ->

pop2imap[2] im cronjob ->

dovecoat ->

Mailclient

1: https://github.com/sarchar/PyBitmessage

2: http://www.linux-france.org/prj/pop2imap/

Ich distanziere mich von diesem absurden Setup

Das Ergebnis wäre:
BM als Mail empfangen per imap-dovecoat
Mail als BM senden per POP-PyBitmessage