CryptoMessenger

Florian “Florob” Zeitz

2014-04-24

Gliederung

Über mich

- Florian Zeitz
- M. Sc. Elektrotechnik/Informationstechnik/Technische Informatik
- XSF Mitglied seit Februar 2010

Über mich

- Florian Zeitz
- M. Sc. Elektrotechnik/Informationstechnik/Technische Informatik
- XSF Mitglied seit Februar 2010

Über mich

- Florian Zeitz
- M. Sc. Elektrotechnik/Informationstechnik/Technische Informatik
- XSF Mitglied seit Februar 2010

Gliederung

CryptoMmessenger

Definition

Eine Instant Messaging Anwendung die über übliche Transportverschlüsselung hinaus weitere Kryptographische Primitive benutzt um die Privatsphäre des Nutzers zu schützen.

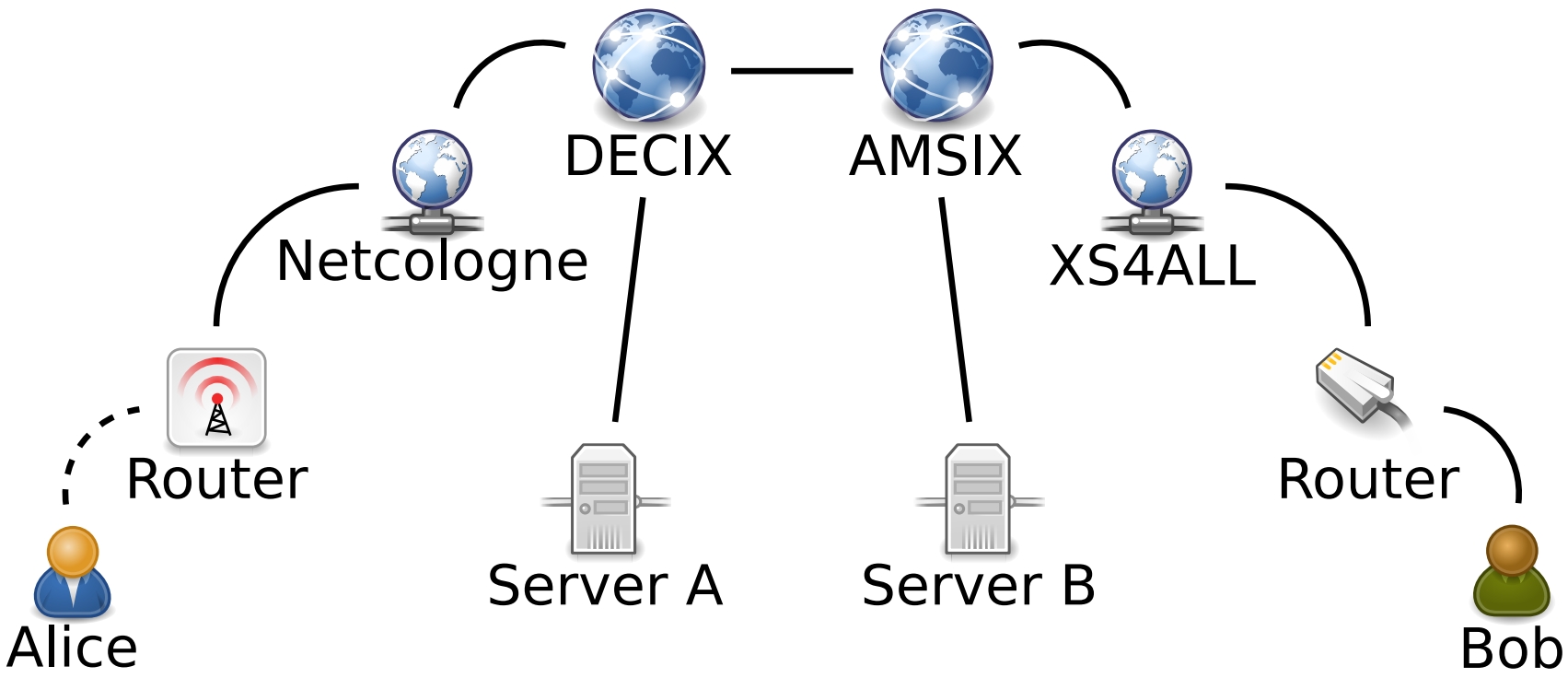
- Verschlüsselung zwischen Client und Server ist mittlerweile üblich
- Verschlüsselung zwischen Clients wird seit den Snowden Enthüllungen verstärkt angepriesen

Gliederung

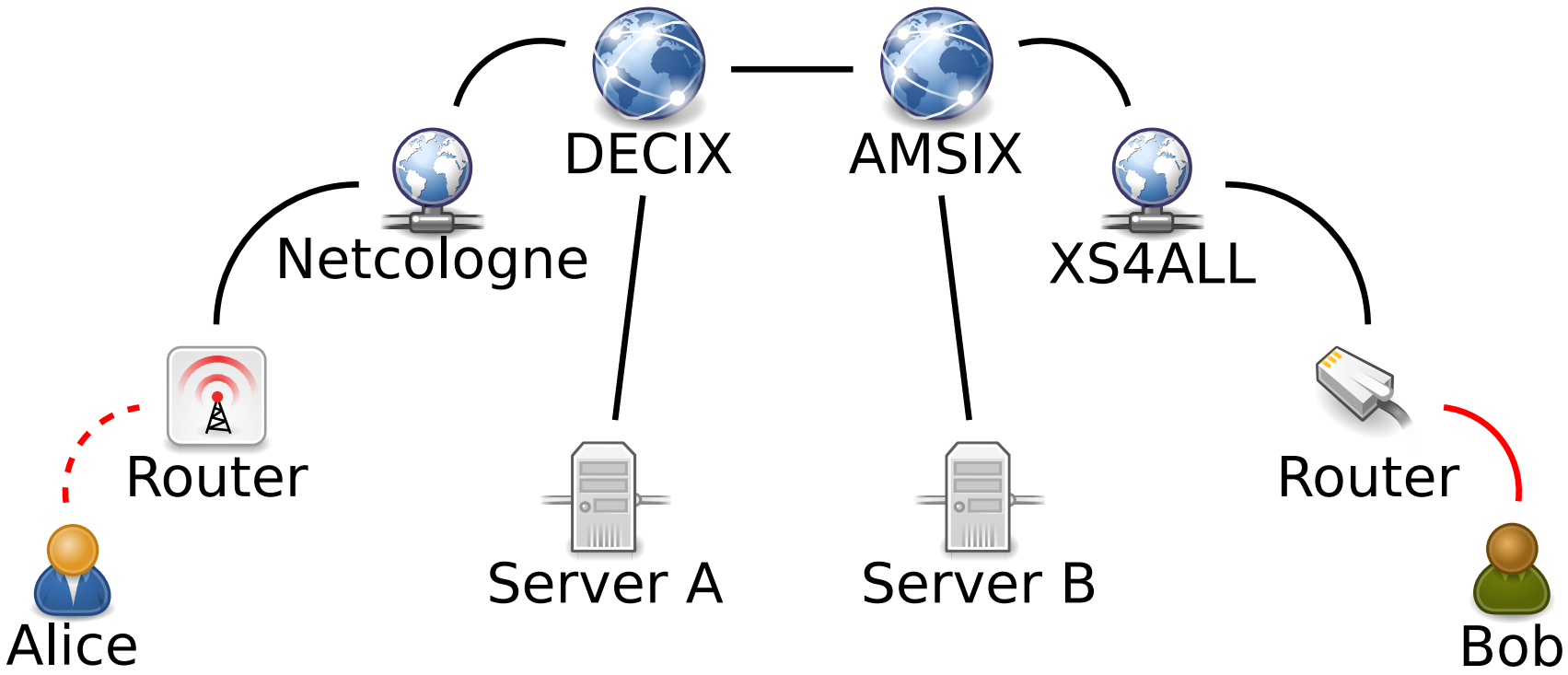
Threat modelling

- Beschreibt eine Bedrohung
- zwei Arten
  1. Beschreibt die Fähigkeiten eines Angreifers, bezogen auf ein Szenario/Protokoll
  2. Beschreibt mögliche Angriffe auf eine konkrete Anwendung, beinhaltet Risikoabschätzung

Generelles Szenario

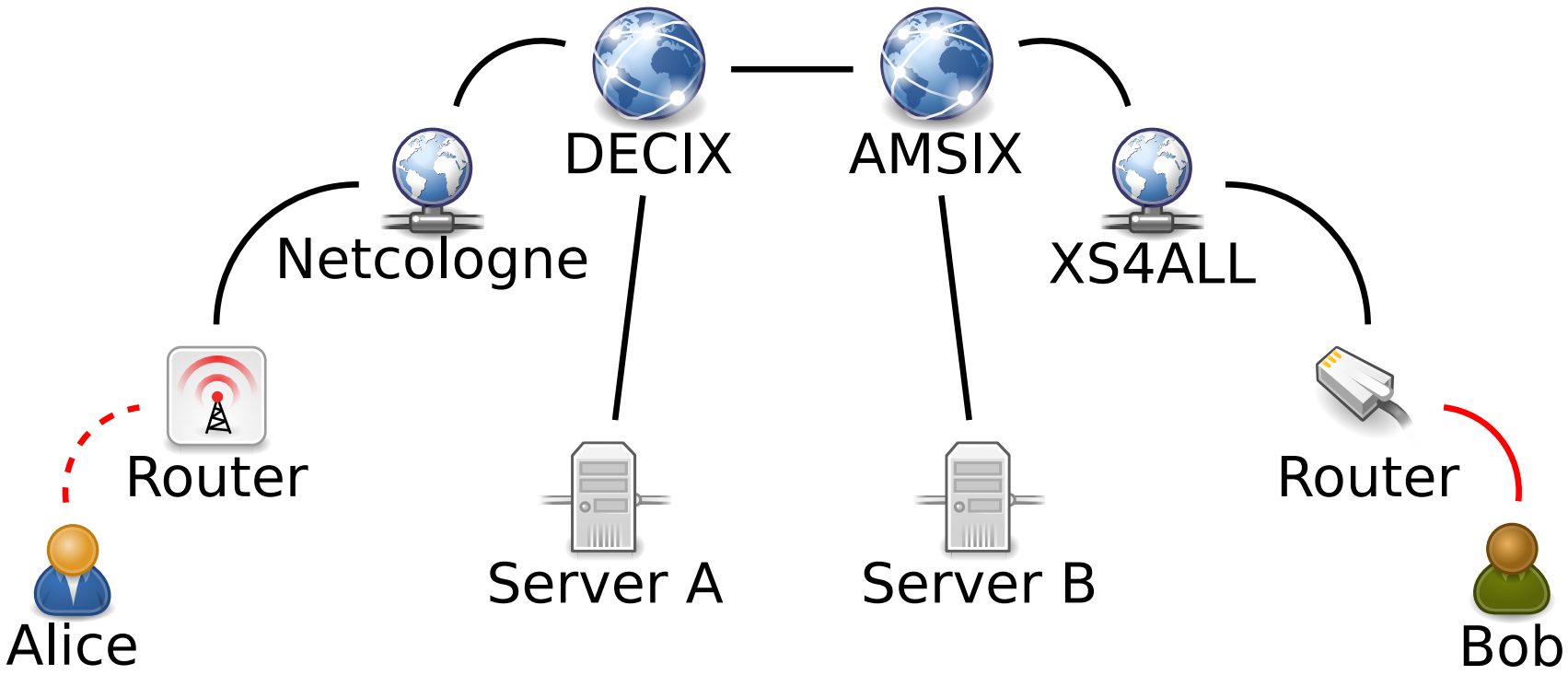


Passive Eavesdropper (Eve)



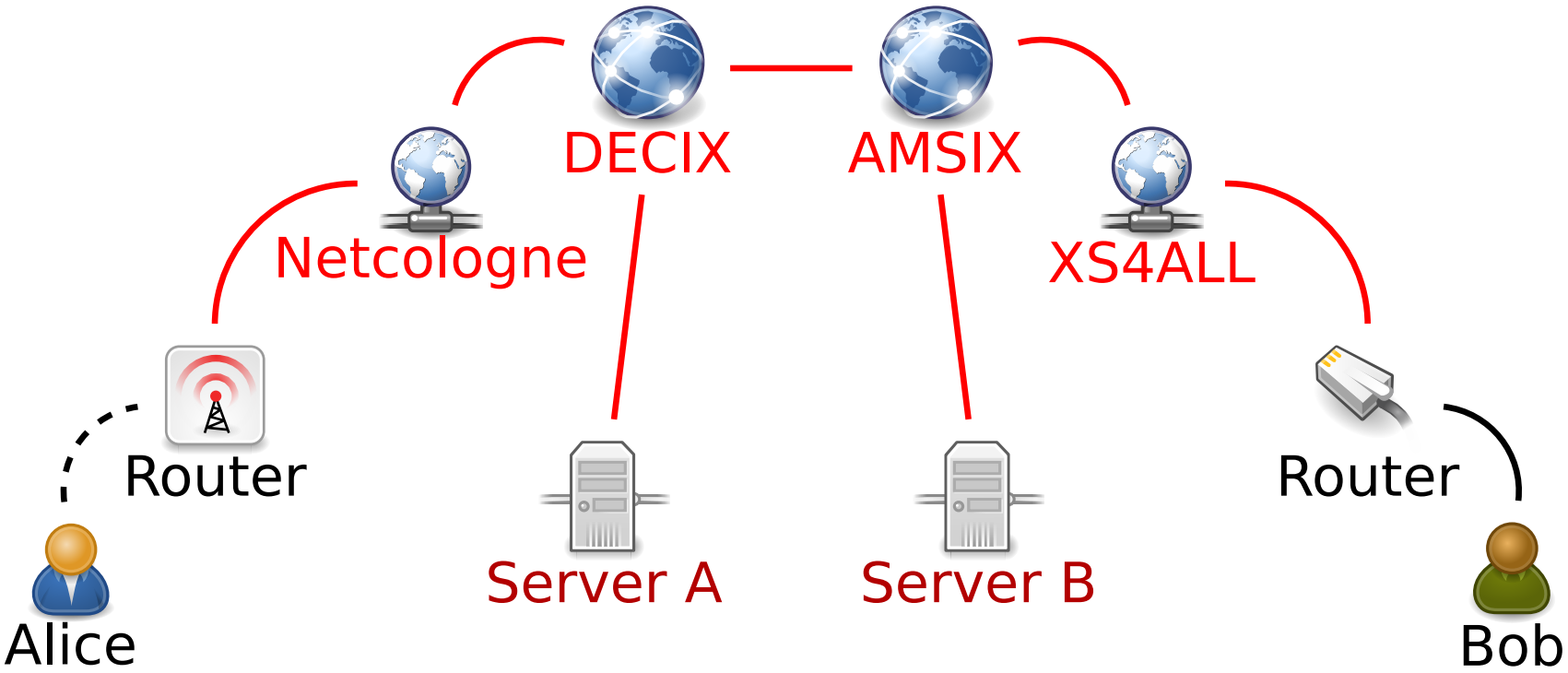
- liest Verbindungen rein passiv mit (WLAN, Ethernet Hub, ARP Poisoning)

Aktiver MITM (Mallior)



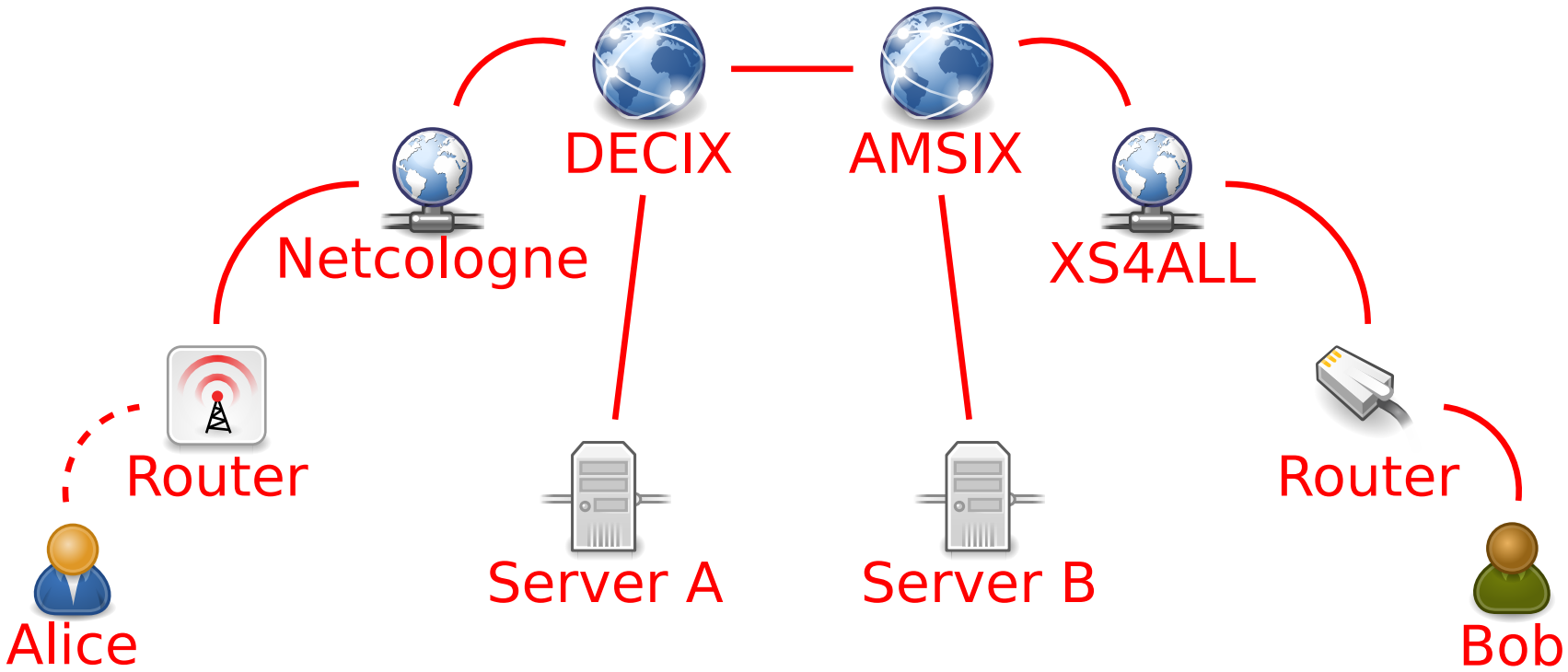
- verändert, blockiert, fälscht Daten (ARP Poisoning, gefälschter AP, ...)

Pervasive Passive Attacker



- modelliert nach XKEYSCORE, Tempora, MUSCULAR
- sieht jedes Paket, an jedem Hop, auf jedem Pfad
- nachträgliche Analyse
- eigene Server kompromittiert?

Gezielter Angriff



- Personenbezogen
- Einbruch in Wohnungen
- Wanzen

Gliederung

Allgemein

- Vertraulichkeit
- Integrität
- Authentizität

(Perfect) Forward Secrecy

- Das ermitteln eines langlebigen Schlüssels kompromittiert nicht alle bisherigen Gespräche
- Sitzungs-/Nachrichtenschlüssel berechnen sich nicht sofort aus private Key
- Schlüssel werden rotiert

(Non-)Repudiation

- repudiation/plausible deniability: Im Nachhinein ist nicht prüfbar wer eine Nachricht erstellt hat
- für rechtliche Angelegenheiten (z. B. in Firmen) ist oft non-repudiation wünschenswert
- der Empfänger sollte trotzdem zum Zeitpunkt des Empfanges wissen wer der Absender war

Verbergen des sozialen Graph

- Metadaten sind wichtig
- oft ist wer mit wem Kontakt hat genau so interessant wie der Inhalt
- schwer, da es das routen behindert

Open-Source vs. proprietär

- OpenSource
  - inhärent auditierbar
  - wird das behauptete auch Implementiert?
  - wer schaut es sich tatsächlich an?
- proprietär
  - reine Vertrauensbasis
  - security by obscurity

Kerkhoffs' Prinzip

Das System darf keine Geheimhaltung erfordern

Gliederung

XMPP

- eXtensible Messaging and Presence Protocol
- offenes Protokoll für Instant Messaging (RFC 6120, 6121, 6122)
- Server zentrisch
- verteilt (mehrere unabhängige, verbundene Server)

XMPP — What you should get

- erzwungenes TLS
- SCRAM-SHA1 — gegenseitige Authentifizierung zwischen Client und Server
- SCRAM-SHA1-PLUS — channel binding, erfolgreiche Authentifizierung $\Rightarrow$ kein TLS MITM
- XEP-0045 — Multi-User Chat
- XEP-0198 — Sitzung Wiederaufnahme nach Netzwerktrennung

XMPP — What you usually get

- erzwungenes TLS
- SCRAM-SHA1 — gegenseitige Authentifizierung zwischen Client und Server
- SCRAM-SHA1-PLUS — channel binding, erfolgreiche Authentifizierung $\Rightarrow$ kein TLS MITM
- XEP-0045 — Multi-User Chat
- XEP-0198 — Sitzung Wiederaufnahme nach Netzwerktrennung

NaCl/libsodium

- Cryptography Bibliothek von Daniel J. Bernstein (djb)
- libsodium — paketierbarer Fork mit kompatibler API
- ein Algorithmus pro Anwendungsfall
- public domain
- Anwendungen benutzen die crypto_box() API für public-key Kryptographie
- Verwendete Suite ist Curve25519-XSalsa20-Poly1305 (alles djb eigen)

NaCl — Curve25519

- key negotiation
- eigentlich ECDH über Curve25519

NaCl — XSalsa20

- Stromchiffre (stream cipher)
- Salsa20 Variante
- Kryptoanalyse als Teil des eSTREAM Projektes

NaCl — Poly1305

- Message Authentication Code
- Variante von Poly1305-AES, über XSalsa20
- beweisbar so sicher wie der zugrundeliegende Chiffre

NaCl — Curve25519-XSalsa20-Poly1305

- Eigenschaften
  - forward secrecy, abhängig vom konkreten Einsatz
  - repudiability durch Konstruktion von Poly1305

OTR

- Off-the-Record Messaging
- Kryptographisches Protokoll für Instant Messaging
- bietet forward secrecy, repudiation
- relativ verbreitet

Gliederung

Red flags

- “highest encryption”
- “ultimate privacy”
- “military grade encryption”
- “100% secure”
- keine Details über verwendete Algorithmen (“n-bit Kryptographie” zählt nicht)

Threema

- proprietär
- kostenpflichtig (< 2€)
- Android und iOS
- Protokoll nicht spezifiziert (manche Hinweise auf die Kryptographie)
  - Benutzt NaCl
  - Wahrscheinlich Curve25519-XSalsa20-Poly1305
  - könnte anderer MAC als Poly1305 sein: repudiation?
  - keine forward secrecy
- Personen über SMS/E-Mail verifiziert von Threema (Orange)
- persönlich verifiziert (Grün)

Telegram

- OpenSource
- kostenlos
- Android, iOS, 3rd-party Anwendugen für Windows, Windows Phone, Linux, Mac
- Wettbewerb mit Preisgeld
  - Kritik an der Form
  - kann auch von sehr unsicheren Protokollen bestanden werden (Moxie Marlinspike)
- argumentum ad verecundiam: “We have Math PhDs”

Telegram

- dokumentiertes Protokoll MTProto
  - selbst entwickelte Kryptographie
  - AES-256-IGE (obskurer Modus, AE mit unsichererer Authentifizierung)
  - SHA-1
  - MAC and Encrypt
  - “If their protocol is secure, it is so by accident, not because of good design” – Taylor Hornby
  - Authentifizierung nur durch den Server?

Heml.is

- open source? “as much as possible”
- kostenlos
- Android und iOS
- crowd-funding
- noch in Entwicklung, nicht öffentlich
- nur ihr eigener Server
- “The way to make the system secure is that we can control the infrastructure”
- “Distributing to other servers makes it impossible to give any guarantees about the security”

Heml.is

- Ursprünglicher Plan: XMPP + PGP
- nutzt libsodium: Curve25519-XSalsa20-Poly1305
- genaues Protokoll nicht spezifiziert – forward secrecy?

TextSecure

- open source
- kostenlos
- Android, iOS (in Entwicklung), 3rd-party Chrome Extension
- Open WhisperSystems (Moxie Marlinspike und co.)
- federated(-ish) (undokumentiert)
- ursprünglich SMS Anwendung, jetzt (auch) IM

TextSecure

- dokumentiertes Protokoll
  - ähnlich zu OTR
  - forward secrecy
  - plausible deniability
  - ECDHE über Curve25519
  - AES-256-CTR
  - HMAC-SHA256

Tox

- open source
- kostenlos
- Android (very alpha), iOS (alpha), Windows, Linux, MacOS X
- kein Server
- dokumentiertes Protokoll (mit viel Interpolation)
  - Curve25519-XSalsa20-Poly1305
  - DHT, sehr ähnlich dem von BitTorrent

Cryptocat

- open source
- kostenlos
- iOS, Android (in Entwicklung), Browser extensions (Firefox, Chrome, Safari, Opera), MacOS X (WebView)
- primär multi-party chat
- in der Vergangenheit viele Sicherheitlücken
- eigene OTR Variante: mpOTR
  - keine repudiability
- normales OTR für private Nachrichten

Cryptocat

- eigenes anwendungsbezogenens Threat Model
- aus dem Open Technology Fund bezahlte Audits
  - Funde, aber weniger kritisch als vor einem Jahr
- Usability (UI/UX) Analyse
  - interessante Ergebnisse: z. B. der Begriff “Fingerprint” erschrickt Nutzer: “Das sollte ich nicht sehen können!”

SilentText/SilentCircle

- proprietär (ältere Versionen als open source)
- kostenlos, aber Abo zur Nutzung erforderlich ($9.95/Monat)
- Android, iOS, Windows
- Unternehmen von Phil Zimmermann (PGP)

SilentText/SilentCircle

- eigenes Protokoll SCIMP (Silent Circle Instant Messaging Protocol)
  - open source Implementation
  - Ideen von: OTR, ZRTP, SSMS, Cryptocat
  - viele NIST-spezifizierte Algorithmen
  - forward secrecy (pro Sitzung)
  - über XMPP übertragen

myEnigma

- proprietär (patente, “vertrauen musst du den Entwicklern sowieso”)
- kostenlos
- Android, iOS, BlackBerry
- eigenes Protokoll
  - DHE mit 2048-bit $\Rightarrow$ forward secrecy, wechselt alle 3,5 Tage
  - AES-256
  - “standard HMAC” (welcher Hash?)
  - HMAC nur für Integrität
    - original Nachricht, aber von wem?
    - vertrauen in den Server

Danke für die Aufmerksamkeit

Fragen?