EOF

Die erste Vorstellung

Nico -telmich- Schottelius

5. September 2007

Einleitung
- Vorstellung
- Motivation
- Über diesen Vortrag

Alternativen
- IRC+SSL
- SILC
- Jabber
- Tor

EOF
- Projektaufbau
- Grundideen
- Beispiele
- Stand

Erste Vorstellung

- Erste Präsentation
- Hier im CCCZH
- Kreative Köpfe
- Kritik bekommen
- Anregen zum Mitdenken und -machen

Erste Vorstellung

- Erste Präsentation
- Hier im CCCZH
- Kreative Köpfe
- Kritik bekommen
- Anregen zum Mitdenken und -machen

Erste Vorstellung

- Erste Präsentation
- Hier im CCCZH
- Kreative Köpfe
- Kritik bekommen
- Anregen zum Mitdenken und -machen

Erste Vorstellung

- Erste Präsentation
- Hier im CCCZH
- Kreative Köpfe
- Kritik bekommen
- Anregen zum Mitdenken und -machen

Erste Vorstellung

- Erste Präsentation
- Hier im CCCZH
- Kreative Köpfe
- Kritik bekommen
- Anregen zum Mitdenken und -machen

!eof

- Junge Hackergruppe
- 2001 gegründet
- Fokus auf Freundlichkeit
- Deutschland, Niederlande, Schweiz
- IRCNet: !eof
- https://www.eof.name/

!eof

- Junge Hackergruppe
- 2001 gegründet
- Fokus auf Freundlichkeit
- Deutschland, Niederlande, Schweiz
- IRCNet: !eof
- https://www.eof.name/

!eof

- Junge Hackergruppe
- 2001 gegründet
- Fokus auf Freundlichkeit
- Deutschland, Niederlande, Schweiz
- IRCNet: !eof
- https://www.eof.name/

!eof

- Junge Hackergruppe
- 2001 gegründet
- Fokus auf Freundlichkeit
- Deutschland, Niederlande, Schweiz
- IRCNet: !eof
- https://www.eof.name/

!eof

- Junge Hackergruppe
- 2001 gegründet
- Fokus auf Freundlichkeit
- Deutschland, Niederlande, Schweiz
- IRCNet: !eof
- https://www.eof.name/

!eof

- Junge Hackergruppe
- 2001 gegründet
- Fokus auf Freundlichkeit
- Deutschland, Niederlande, Schweiz
- IRCNet: !eof
- https://www.eof.name/

Nico Schottelius

- Entwickelt freie, quelloffene Software (FOSS)
- Philosophie: Machen statt meckern
- aka telmich
- https://nico.schottelius.org/

Nico Schottelius

- Entwickelt freie, quelloffene Software (FOSS)
- Philosophie: Machen statt meckern
- aka telmich
- https://nico.schottelius.org/

Nico Schottelius

- Entwickelt freie, quelloffene Software (FOSS)
- Philosophie: Machen statt meckern
- aka telmich
- https://nico.schottelius.org/

Nico Schottelius

- Entwickelt freie, quelloffene Software (FOSS)
- Philosophie: Machen statt meckern
- aka telmich
- https://nico.schottelius.org/

EOF

- Alternatives Chatsystem
- Projekt von !eof

EOF

- Alternatives Chatsystem
- Projekt von !eof

Warum dieser Vortrag?

- Idee vorstellen
- Kritik bekommen
- Werben von
  - Entwicklern
  - Testern
  - (noch) nicht Benutzern

Warum dieser Vortrag?

- Idee vorstellen
- Kritik bekommen
- Werben von
  - Entwicklern
  - Testern
  - (noch) nicht Benutzern

Warum dieser Vortrag?

- Idee vorstellen
- Kritik bekommen
- Werben von
  - Entwicklern
  - Testern
  - (noch) nicht Benutzern

Warum dieser Vortrag?

- Idee vorstellen
- Kritik bekommen
- Werben von
  - Entwicklern
  - Testern
  - (noch) nicht Benutzern

Warum dieser Vortrag?

- Idee vorstellen
- Kritik bekommen
- Werben von
  - Entwicklern
  - Testern
  - (noch) nicht Benutzern

Warum dieser Vortrag?

- Idee vorstellen
- Kritik bekommen
- Werben von
  - Entwicklern
  - Testern
  - (noch) nicht Benutzern

Warum das Rad neu erfinden?

- IRC ist grundsätzlich unverschlüsselt
- Suchen eine generell nicht abhörbare Alternative
- Existierende Alternativen erfüllen nicht alle Anforderungen

Warum das Rad neu erfinden?

- IRC ist grundsätzlich unverschlüsselt
- Suchen eine generell nicht abhörbare Alternative
- Existierende Alternativen erfüllen nicht alle Anforderungen

Warum das Rad neu erfinden?

- IRC ist grundsätzlich unverschlüsselt
- Suchen eine generell nicht abhörbare Alternative
- Existierende Alternativen erfüllen nicht alle Anforderungen

Anforderungen

- Dezentralität
  - Ohne zentralen Server
- Nicht abhörbar
  - **Wer** mit **wem wann was** redet
- Verschlüsselung und Signatur

Anforderungen

- Dezentralität
  - Ohne zentralen Server
- Nicht abhörbar
  - **Wer** mit **wem** **wann** **was** redet
- Verschlüsselung und Signatur

Anforderungen

- Dezentralität
  - Ohne zentralen Server
- Nicht abhörbar
  - **Wer** mit **wem** **wann** **was** redet
- Verschlüsselung und Signatur

Anforderungen

- Dezentralität
  - Ohne zentralen Server
- Nicht abhörbar
  - **Wer** mit **wem wann was** redet
- Verschlüsselung und Signatur

Anforderungen

- Dezentralität
  - Ohne zentralen Server
- Nicht abhörbar
  - **Wer** mit **wem wann was** redet
- Verschlüsselung und Signatur

Versionen dieses Vortrages

- Nur Text (LaTeX oder PDF)
- Nur Ton (Aufnahme in Ogg)
- Text und Ton (Theora-Video)

Versionen dieses Vortrages

- Nur Text (LaTeX oder PDF)
- Nur Ton (Aufnahme in Ogg)
- Text und Ton (Theora-Video)

Versionen dieses Vortrages

- Nur Text (LaTeX oder PDF)
- Nur Ton (Aufnahme in Ogg)
- Text und Ton (Theora-Video)

Kopieren dieses Vortrages

- Ist (hiermit) explizit gestattet
- Creative Commons Attribution-Share Alike 2.0 Germany License
- http://creativecommons.org/licenses/by-sa/2.0/de/

Kopieren dieses Vortrages

- Ist (hiermit) explizit gestattet
- Creative Commons Attribution-Share Alike 2.0 Germany License
- http://creativecommons.org/licenses/by-sa/2.0/de/

Kopieren dieses Vortrages

- Ist (hiermit) explizit gestattet
- Creative Commons Attribution-Share Alike 2.0 Germany License
- http://creativecommons.org/licenses/by-sa/2.0/de/

Quellen dieses Vortrages

- Unter folgenden Adressen zu finden:
  - https://nico.schottelius.org/projects/eof-1/
  - https://www.eof.name/projects/eof-1/

Quellen dieses Vortrages

- Unter folgenden Adressen zu finden:
  - https://nico.schottelius.org/projects/eof-1/
  - https://www.eof.name/projects/eof-1/

Quellen dieses Vortrages

- Unter folgenden Adressen zu finden:
  - https://nico.schottelius.org/projects/eof-1/
  - https://www.eof.name/projects/eof-1/

Übersicht IRC+SSL

- Standard IRC mit SSL
- Verschlüsselung
  - Client zum Server
  - Server zum Server
- „Nur SSL“-Räume

Übersicht IRC+SSL

- Standard IRC mit SSL
- Verschlüsselung
  - Client zum Server
  - Server zum Server
- „Nur SSL“-Räume

Übersicht IRC+SSL

- Standard IRC mit SSL
- Verschlüsselung
  - Client zum Server
  - Server zum Server
- „Nur SSL“-Räume

Übersicht IRC+SSL

- Standard IRC mit SSL
- Verschlüsselung
  - Client zum Server
  - Server zum Server
- „Nur SSL“-Räume

Vorteile

- Erprobtes Protokoll
- Stabile Software vorhanden
- Verschlüsselung ist einfach hinzufügbar

Vorteile

- Erprobtes Protokoll
- Stabile Software vorhanden
- Verschlüsselung ist einfach hinzufügbar

Vorteile

- Erprobtes Protokoll
- Stabile Software vorhanden
- Verschlüsselung ist einfach hinzufügbar

Nachteile

- Innerhalb der Server ungesichert
  - Kompromitierung durch Übernahme eines Servers möglich
- Keine Ende-zu-Ende-Verschlüsselung
- Teile der Verbindung können unverschlüsselt sein
- Statistische Analyse möglich
  - Wer sendet wann, wer empfängt wann?

Nachteile

- Innerhalb der Server ungesichert
  - Kompromitierung durch Übernahme eines Servers möglich
- Keine Ende-zu-Ende-Verschlüsselung
- Teile der Verbindung können unverschlüsselt sein
- Statistische Analyse möglich
  - Wer sendet wann, wer empfängt wann?

Nachteile

- Innerhalb der Server ungesichert
  - Kompromitierung durch Übernahme eines Servers möglich
- Keine Ende-zu-Ende-Verschlüsselung
- Teile der Verbindung können unverschlüsselt sein
- Statistische Analyse möglich
  - Wer sendet wann, wer empfängt wann?

Nachteile

- Innerhalb der Server ungesichert
  - Kompromitierung durch Übernahme eines Servers möglich
- Keine Ende-zu-Ende-Verschlüsselung
- Teile der Verbindung können unverschlüsselt sein
- Statistische Analyse möglich
  - Wer sendet wann, wer empfängt wann?

Nachteile

- Innerhalb der Server ungesichert
  - Kompromitierung durch Übernahme eines Servers möglich
- Keine Ende-zu-Ende-Verschlüsselung
- Teile der Verbindung können unverschlüsselt sein
- Statistische Analyse möglich
  - Wer sendet wann, wer empfängt wann?

Nachteile

- Innerhalb der Server ungesichert
  - Kompromitierung durch Übernahme eines Servers möglich
- Keine Ende-zu-Ende-Verschlüsselung
- Teile der Verbindung können unverschlüsselt sein
- Statistische Analyse möglich
  - Wer sendet wann, wer empfängt wann?

Übersicht SILC

- **S**ecure **I**nternet **L**ive **C**hat
- Geplanter Ersatz für IRC
- Verschlüsselung
  - Server zum Server
  - Client zum Server
  - Client zum Client
- http://www.silcnet.org/

Übersicht SILC

- **S**ecure **I**nternet **L**ive **C**hat
- Geplanter Ersatz für IRC
- Verschlüsselung
  - Server zum Server
  - Client zum Server
  - Client zum Client
- http://www.silcnet.org/

Übersicht SILC

- **S**ecure **I**nternet **L**ive **C**hat
- Geplanter Ersatz für IRC
- Verschlüsselung
  - Server zum Server
  - Client zum Server
  - Client zum Client
- http://www.silcnet.org/

Übersicht SILC

- **S**ecure **I**nternet **L**ive **C**hat
- Geplanter Ersatz für IRC
- Verschlüsselung
  - Server zum Server
  - Client zum Server
  - Client zum Client
- http://www.silcnet.org/

Übersicht SILC

- **S**ecure **I**nternet **L**ive **C**hat
- Geplanter Ersatz für IRC
- Verschlüsselung
  - Server zum Server
  - Client zum Server
  - Client zum Client
- http://www.silcnet.org/

Übersicht SILC

- **S**ecure **I**nternet **L**ive **C**hat
- Geplanter Ersatz für IRC
- Verschlüsselung
  - Server zum Server
  - Client zum Server
  - Client zum Client
- http://www.silcnet.org/

Übersicht SILC

- **S**ecure **I**nternet **L**ive **C**hat
- Geplanter Ersatz für IRC
- Verschlüsselung
  - Server zum Server
  - Client zum Server
  - Client zum Client
- http://www.silcnet.org/

Vorteile

- Verschlüsselung von Anfang eingeplant
- Integration in einen bekannten Chat-Client (irssi)

Vorteile

- Verschlüsselung von Anfang eingeplant
- Integration in einen bekannten Chat-Client (irssi)

Nachteile

- Instabile Software
  - Client stürzt ab
  - Server verliert Kanal-Parameter (z.B. +r)
  - Server verliert Kanäle
- Eigenes (unerforschtes) Protokoll
- Statistische Analyse möglich

Nachteile

- Instabile Software
  - Client stürzt ab
  - Server verliert Kanal-Parameter (z.B. +r)
  - Server verliert Kanäle
- Eigenes (unerforschtes) Protokoll
- Statistische Analyse möglich

Nachteile

- Instabile Software
  - Client stürzt ab
  - Server verliert Kanal-Parameter (z.B. +r)
  - Server verliert Kanäle
- Eigenes (unerforschtes) Protokoll
- Statistische Analyse möglich

Nachteile

- Instabile Software
  - Client stürzt ab
  - Server verliert Kanal-Parameter (z.B. +r)
  - Server verliert Kanäle
- Eigenes (unerforschtes) Protokoll
- Statistische Analyse möglich

Nachteile

- Instabile Software
  - Client stürzt ab
  - Server verliert Kanal-Parameter (z.B. +r)
  - Server verliert Kanäle
- Eigenes (unerforschtes) Protokoll
- Statistische Analyse möglich

Nachteile

- Instabile Software
  - Client stürzt ab
  - Server verliert Kanal-Parameter (z.B. +r)
  - Server verliert Kanäle
- Eigenes (unerforschtes) Protokoll
- Statistische Analyse möglich

Übersicht Jabber

- Instant messaging (IM) Protokoll
- Transport via XML

Übersicht Jabber

- Instant messaging (IM) Protokoll
- Transport via XML

Vorteile

- Viele Clients verfügbar

Nachteile

- Kanäle sind eine Erweiterung
- Verschlüsselung optional
- Statistische Analyse möglich

Nachteile

- Kanäle sind eine Erweiterung
- Verschlüsselung optional
- Statistische Analyse möglich

Nachteile

- Kanäle sind eine Erweiterung
- Verschlüsselung optional
- Statistische Analyse möglich

Übersicht Tor

- Anonymisierungsdienst
- Kein Chatprotokoll
- Zwiebelprinzip

Übersicht Tor

- Anonymisierungsdienst
- Kein Chatprotokoll
- Zwiebelprinzip

Übersicht Tor

- Anonymisierungsdienst
- Kein Chatprotokoll
- Zwiebelprinzip

Vorteile

- Stabile Software vorhanden

Nachteile

- Client sendet nur wenn er wirklich sendet
  - Statistische Analyse möglich
- Empfänger sendet Paket nicht weiter
  - Endpunkte sind erkennbar

Nachteile

- Client sendet nur wenn er wirklich sendet
  - Statistische Analyse möglich
- Empfänger sendet Paket nicht weiter
  - Endpunkte sind erkennbar

Nachteile

- Client sendet nur wenn er wirklich sendet
  - Statistische Analyse möglich
- Empfänger sendet Paket nicht weiter
  - Endpunkte sind erkennbar

Nachteile

- Client sendet nur wenn er wirklich sendet
  - Statistische Analyse möglich
- Empfänger sendet Paket nicht weiter
  - Endpunkte sind erkennbar

EOF

- Projektaufbau
- Grundideen
- Beispiele
- Stand

EOF

- Projektaufbau
- Grundideen
- Beispiele
- Stand

EOF

- Projektaufbau
- Grundideen
- Beispiele
- Stand

EOF

- Projektaufbau
- Grundideen
- Beispiele
- Stand

Evolution

- Kleine Teile programmieren
- Vorschläge für Protokolle entwerfen
- Ausprobieren und aus Fehlern lernen

Evolution

- Kleine Teile programmieren
- Vorschläge für Protokolle entwerfen
- Ausprobieren und aus Fehlern lernen

Evolution

- Kleine Teile programmieren
- Vorschläge für Protokolle entwerfen
- Ausprobieren und aus Fehlern lernen

EOF-1

- Erste Phase
- Ideen dokumentieren
- Ideen diskutieren
- Viele Fehler machen
- Juli 2007 bis Dezember 2007

EOF-1

- Erste Phase
- Ideen dokumentieren
- Ideen diskutieren
- Viele Fehler machen
- Juli 2007 bis Dezember 2007

EOF-1

- Erste Phase
- Ideen dokumentieren
- Ideen diskutieren
- Viele Fehler machen
- Juli 2007 bis Dezember 2007

EOF-1

- Erste Phase
- Ideen dokumentieren
- Ideen diskutieren
- Viele Fehler machen
- Juli 2007 bis Dezember 2007

EOF-1

- Erste Phase
- Ideen dokumentieren
- Ideen diskutieren
- Viele Fehler machen
- Juli 2007 bis Dezember 2007

EOF-1 Vorgehen

- Spezifikationsentwürfe schreiben für
  - Protokolle
  - Software
- Freie Wahl der Programmiersprache
  - Kommunikation über klar definierte Schnittstellen
- Modularer Aufbau

EOF-1 Vorgehen

- Spezifikationsentwürfe schreiben für
  - Protokolle
  - Software
- Freie Wahl der Programmiersprache
  - Kommunikation über klar definierte Schnittstellen
- Modularer Aufbau

EOF-1 Vorgehen

- Spezifikationsentwürfe schreiben für
  - Protokolle
  - Software
- Freie Wahl der Programmiersprache
  - Kommunikation über klar definierte Schnittstellen
- Modularer Aufbau

EOF-1 Vorgehen

- Spezifikationsentwürfe schreiben für
  - Protokolle
  - Software
- Freie Wahl der Programmiersprache
  - Kommunikation über klar definierte Schnittstellen
- Modularer Aufbau

EOF-1 Vorgehen

- Spezifikationsentwürfe schreiben für
  - Protokolle
  - Software
- Freie Wahl der Programmiersprache
  - Kommunikation über klar definierte Schnittstellen
- Modularer Aufbau

EOF-1 Vorgehen

- Spezifikationsentwürfe schreiben für
  - Protokolle
  - Software
- Freie Wahl der Programmiersprache
  - Kommunikation über klar definierte Schnittstellen
- Modularer Aufbau

EOF-2

- Fehler aus EOF-1 korrigieren
- Dokumentation erstellen
- Plan für finale Version erstellen
- Januar 2008 bis Juni 2008

EOF-2

- Fehler aus EOF-1 korrigieren
- Dokumentation erstellen
- Plan für finale Version erstellen
- Januar 2008 bis Juni 2008

EOF-2

- Fehler aus EOF-1 korrigieren
- Dokumentation erstellen
- Plan für finale Version erstellen
- Januar 2008 bis Juni 2008

EOF-2

- Fehler aus EOF-1 korrigieren
- Dokumentation erstellen
- Plan für finale Version erstellen
- Januar 2008 bis Juni 2008

EOF-3

- Spezifikation von EOF-2 implementieren
- Unterstützung mehrerer Betriebsysteme
- Produktiv nutzbar
- Juli 2008 bis Dezember 2008

EOF-3

- Spezifikation von EOF-2 implementieren
- Unterstützung mehrerer Betriebsysteme
- Produktiv nutzbar
- Juli 2008 bis Dezember 2008

EOF-3

- Spezifikation von EOF-2 implementieren
- Unterstützung mehrerer Betriebsysteme
- Produktiv nutzbar
- Juli 2008 bis Dezember 2008

EOF-3

- Spezifikation von EOF-2 implementieren
- Unterstützung mehrerer Betriebsysteme
- Produktiv nutzbar
- Juli 2008 bis Dezember 2008

Modularität

- Viele kleine Teile
- Alles ist austauschbar
- Klar definierte Schnittstellen
- Für anderes wiederverwendbar

Modularität

- Viele kleine Teile
- Alles ist austauschbar
- Klar definierte Schnittstellen
- Für anderes wiederverwendbar

Modularität

- Viele kleine Teile
- Alles ist austauschbar
- Klar definierte Schnittstellen
- Für anderes wiederverwendbar

Modularität

- Viele kleine Teile
- Alles ist austauschbar
- Klar definierte Schnittstellen
- Für anderes wiederverwendbar

Das Zwiebelprinzip

- Mehrfach verschlüsselt
- Nie direkt an den Empfänger senden
- Auch der Empfänger sendet es weiter!

Das Zwiebelprinzip

- Mehrfach verschlüsselt
- Nie direkt an den Empfänger senden
- Auch der Empfänger sendet es weiter!

Das Zwiebelprinzip

- Mehrfach verschlüsselt
- Nie direkt an den Empfänger senden
- Auch der Empfänger sendet es weiter!

Indirekte Kommunikation

- Über mehrere Stationen
- Jede Station ent- und verschlüsselt
- Keine Station sendet direkt an den End-Empfänger

Indirekte Kommunikation

- Über mehrere Stationen
- Jede Station ent- und verschlüsselt
- Keine Station sendet direkt an den End-Empfänger

Indirekte Kommunikation

- Über mehrere Stationen
- Jede Station ent- und verschlüsselt
- Keine Station sendet direkt an den End-Empfänger

Alles verschlüsselt

- Kein unverschlüsseltes Paket
- Initialer Schlüsseltausch über sichere Kanäle
- Schlüsseltausch später über etablierten Kanal

Alles verschlüsselt

- Kein unverschlüsseltes Paket
- Initialer Schlüsseltausch über sichere Kanäle
- Schlüsseltausch später über etablierten Kanal

Alles verschlüsselt

- Kein unverschlüsseltes Paket
- Initialer Schlüsseltausch über sichere Kanäle
- Schlüsseltausch später über etablierten Kanal

Nachrichten signiert

- Sicherstellen, dass ich mit dem richtigen kommuniziere
- Signatur ist nur sichbar für den Empfänger

Nachrichten signiert

- Sicherstellen, dass ich mit dem richtigen kommuniziere
- Signatur ist nur sichbar für den Empfänger

Abstraktion vom Transportprotokoll

- Übertragung ist **nicht** Bestandteil von EOF
- Das Paketformat wird unabhängig vom Transportprotkoll definiert
- Beliebige Protokolle möglich
- Einfaches Tunneln von Firewalls
  - z.B. direkte „HTTP-Verbindung“ oder via Webforen

Abstraktion vom Transportprotokoll

- Übertragung ist **nicht** Bestandteil von EOF
- Das Paketformat wird unabhängig vom Transportprotkoll definiert
- Beliebige Protokolle möglich
- Einfaches Tunneln von Firewalls
  - z.B. direkte „HTTP-Verbindung“ oder via Webforen

Abstraktion vom Transportprotokoll

- Übertragung ist **nicht** Bestandteil von EOF
- Das Paketformat wird unabhängig vom Transportprotkoll definiert
- Beliebige Protokolle möglich
- Einfaches Tunneln von Firewalls
  - z.B. direkte „HTTP-Verbindung“ oder via Webforen

Abstraktion vom Transportprotokoll

- Übertragung ist **nicht** Bestandteil von EOF
- Das Paketformat wird unabhängig vom Transportprotkoll definiert
- Beliebige Protokolle möglich
- Einfaches Tunneln von Firewalls
  - z.B. direkte „HTTP-Verbindung“ oder via Webforen

Abstraktion vom Transportprotokoll

- Übertragung ist **nicht** Bestandteil von EOF
- Das Paketformat wird unabhängig vom Transportprotkoll definiert
- Beliebige Protokolle möglich
- Einfaches Tunneln von Firewalls
  - z.B. direkte „HTTP-Verbindung“ oder via Webforen

Rauschen

- Jeder Teilnehmer sendet „immer“ (fixer Intervall)
  - Fest definierter Sendeintervall
  - Wenn nichts zu senden ist werden Zufallsdaten gesendet
  - Zufallsdaten werden genauso wie richtige Pakete behandelt
- Von ausen nicht zu erkennen, wann er wirklich sendet

Rauschen

- Jeder Teilnehmer sendet „immer“ (fixer Intervall)
  - Fest definierter Sendeintervall
  - Wenn nichts zu senden ist werden Zufallsdaten gesendet
  - Zufallsdaten werden genauso wie richtige Pakete behandelt
- Von ausen nicht zu erkennen, wann er wirklich sendet

Rauschen

- Jeder Teilnehmer sendet „immer“ (fixer Intervall)
  - Fest definierter Sendeintervall
  - Wenn nichts zu senden ist werden Zufallsdaten gesendet
  - Zufallsdaten werden genauso wie richtige Pakete behandelt
- Von ausen nicht zu erkennen, wann er wirklich sendet

Rauschen

- Jeder Teilnehmer sendet „immer“ (fixer Intervall)
  - Fest definierter Sendeintervall
  - Wenn nichts zu senden ist werden Zufallsdaten gesendet
  - Zufallsdaten werden genauso wie richtige Pakete behandelt
- Von ausen nicht zu erkennen, wann er wirklich sendet

Rauschen

- Jeder Teilnehmer sendet „immer“ (fixer Intervall)
  - Fest definierter Sendeintervall
  - Wenn nichts zu senden ist werden Zufallsdaten gesendet
  - Zufallsdaten werden genauso wie richtige Pakete behandelt
- Von ausen nicht zu erkennen, wann er wirklich sendet

Beispiele

- Für
  - Ausgewählte Teile von EOF
  - Übliche Handlungen beim Chatten
- Um abstrakte Informationen konkretisieren

Beispiele

- Für
  - Ausgewählte Teile von EOF
  - Übliche Handlungen beim Chatten
- Um abstrakte Informationen konkretisieren

Beispiele

- Für
  - Ausgewählte Teile von EOF
  - Übliche Handlungen beim Chatten
- Um abstrakte Informationen konkretisieren

Beispiele

- Für
  - Ausgewählte Teile von EOF
  - Übliche Handlungen beim Chatten
- Um abstrakte Informationen konkretisieren

Wie man sich findet

- Über Marktschreier
- Marktschreier verwalten Metaninformationen
  - Liste von bekannten Kanälen
  - Liste von bekannten Partner
- Jeder Client kann Marktschreier sein

Wie man sich findet

- Über Marktschreier
- Marktschreier verwalten Metaninformationen
  - Liste von bekannten Kanälen
  - Liste von bekannten Partner
- Jeder Client kann Marktschreier sein

Wie man sich findet

- Über Marktschreier
- Marktschreier verwalten Metaninformationen
  - Liste von bekannten Kanälen
  - Liste von bekannten Partner
- Jeder Client kann Marktschreier sein

Wie man sich findet

- Über Marktschreier
- Marktschreier verwalten Metaninformationen
  - Liste von bekannten Kanälen
  - Liste von bekannten Partner
- Jeder Client kann Marktschreier sein

Wie man sich findet

- Über Marktschreier
- Marktschreier verwalten Metaninformationen
  - Liste von bekannten Kanälen
  - Liste von bekannten Partner
- Jeder Client kann Marktschreier sein

Über die Marktschreier

- Besitzen und Verteilen **nur** öffentliche Informationen
- Verwalten Liste von öffentlichen Kanälen
- Vermitteln Partner zum Indirekten Senden
- Sind ganz normale EOF-Clients
  - Erlauben zusätzlich Abfragen und Speichern von Metainformationen

Über die Marktschreier

- Besitzen und Verteilen **nur** öffentliche Informationen
- Verwalten Liste von öffentlichen Kanälen
- Vermitteln Partner zum Indirekten Senden
- Sind ganz normale EOF-Clients
  - Erlauben zusätzlich Abfragen und Speichern von Metainformationen

Über die Marktschreier

- Besitzen und Verteilen **nur** öffentliche Informationen
- Verwalten Liste von öffentlichen Kanälen
- Vermitteln Partner zum Indirekten Senden
- Sind ganz normale EOF-Clients
  - Erlauben zusätzlich Abfragen und Speichern von Metainformationen

Über die Marktschreier

- Besitzen und Verteilen **nur** öffentliche Informationen
- Verwalten Liste von öffentlichen Kanälen
- Vermitteln Partner zum Indirekten Senden
- Sind ganz normale EOF-Clients
  - Erlauben zusätzlich Abfragen und Speichern von Metainformationen

Über die Marktschreier

- Besitzen und Verteilen **nur** öffentliche Informationen
- Verwalten Liste von öffentlichen Kanälen
- Vermitteln Partner zum Indirekten Senden
- Sind ganz normale EOF-Clients
  - Erlauben zusätzlich Abfragen und Speichern von Metainformationen

Vollstaendige Verschlüsselung

- Öffentlicher Schlüssel wird vorher per
  - PGP verschlüsselter E-Mail
  - Versiegelten Brief
  - Telefon
- ausgetauscht

Vollstaendige Verschlüsselung

- Öffentlicher Schlüssel wird vorher per
  - PGP verschlüsselter E-Mail
  - Versiegelten Brief
  - Telefon
- ausgetauscht

Vollstaendige Verschlüsselung

- Öffentlicher Schlüssel wird vorher per
  - PGP verschlüsselter E-Mail
  - Versiegelten Brief
  - Telefon
- ausgetauscht

Vollstaendige Verschlüsselung

- Öffentlicher Schlüssel wird vorher per
  - PGP verschlüsselter E-Mail
  - Versiegelten Brief
  - Telefon
- ausgetauscht

Beitreten eines Kanals

- Verbinden zum Marktschreier
  - „Was für Kanäle kennst Du?“
  - Liste: „blackhats“ ... „antim$“ ... „EOF-1“ ...
  - „Teile bitte den Leuten von Kanal EOF-1 mit, dass ich beitreten möchte.“
- Marktschreier verbindet sich zu einem Partner, der die anderen kennt
- Der wiederrum schickt Pakete an alle anderen (indirekt) weiter
- Die Kanalinsassen melden sich dann bei mir

Beitreten eines Kanals

- Verbinden zum Marktschreier
  - „Was für Kanäle kennst Du?“
  - Liste: „blackhats“ ... „antim$“ ... „EOF-1“ ...
  - „Teile bitte den Leuten von Kanal EOF-1 mit, dass ich beitreten möchte.“
- Marktschreier verbindet sich zu einem Partner, der die anderen kennt
- Der wiederrum schickt Pakete an alle anderen (indirekt) weiter
- Die Kanalinsassen melden sich dann bei mir

Beitreten eines Kanals

- Verbinden zum Marktschreier
  - „Was für Kanäle kennst Du?“
  - Liste: „blackhats“ ... „antim$“ ... „EOF-1“ ...
  - „Teile bitte den Leuten von Kanal EOF-1 mit, dass ich beitreten möchte.“
- Marktschreier verbindet sich zu einem Partner, der die anderen kennt
- Der wiederrum schickt Pakete an alle anderen (indirekt) weiter
- Die Kanalinsassen melden sich dann bei mir

Beitreten eines Kanals

- Verbinden zum Marktschreier
  - „Was für Kanäle kennst Du?“
  - Liste: „blackhats“ ... „antim$“ ... „EOF-1“ ...
  - „Teile bitte den Leuten von Kanal EOF-1 mit, dass ich beitreten möchte.“
- Marktschreier verbindet sich zu einem Partner, der die anderen kennt
- Der wiederrum schickt Pakete an alle anderen (indirekt) weiter
- Die Kanalinsassen melden sich dann bei mir

Beitreten eines Kanals

- Verbinden zum Marktschreier
  - „Was für Kanäle kennst Du?“
  - Liste: „blackhats“ ... „antim$“ ... „EOF-1“ ...
  - „Teile bitte den Leuten von Kanal EOF-1 mit, dass ich beitreten möchte.“
- Marktschreier verbindet sich zu einem Partner, der die anderen kennt
- Der wiederrum schickt Pakete an alle anderen (indirekt) weiter
- Die Kanalinsassen melden sich dann bei mir

Beitreten eines Kanals

- Verbinden zum Marktschreier
  - „Was für Kanäle kennst Du?“
  - Liste: „blackhats“ ... „antim$“ ... „EOF-1“ ...
  - „Teile bitte den Leuten von Kanal EOF-1 mit, dass ich beitreten möchte.“
- Marktschreier verbindet sich zu einem Partner, der die anderen kennt
- Der wiederrum schickt Pakete an alle anderen (indirekt) weiter
- Die Kanalinsassen melden sich dann bei mir

Beitreten eines Kanals

- Verbinden zum Marktschreier
  - „Was für Kanäle kennst Du?“
  - Liste: „blackhats“ ... „antim$“ ... „EOF-1“ ...
  - „Teile bitte den Leuten von Kanal EOF-1 mit, dass ich beitreten möchte.“
- Marktschreier verbindet sich zu einem Partner, der die anderen kennt
- Der wiederrum schickt Pakete an alle anderen (indirekt) weiter
- Die Kanalinsassen melden sich dann bei mir

Woher wissen die, wie sie mich erreichen?

- Zum Anfang übermittelt man dem Marktschreier, wo man erreichbar ist
- Diese Information leitet er weiter

Woher wissen die, wie sie mich erreichen?

- Zum Anfang übermittelt man dem Marktschreier, wo man erreichbar ist
- Diese Information leitet er weiter

Transport-Protokolle

- Etwas, mit dem man senden und/oder empfangen kann
- Beliebige Protokolle
  - Empfangen via SMTP HELO
  - Senden via Webdav
  - Empfangen via ICQ/Jabber/Skype/...

Transport-Protokolle

- Etwas, mit dem man senden und/oder empfangen kann
- Beliebige Protokolle
  - Empfangen via SMTP HELO
  - Senden via Webdav
  - Empfangen via ICQ/Jabber/Skype/...

Transport-Protokolle

- Etwas, mit dem man senden und/oder empfangen kann
- Beliebige Protokolle
  - Empfangen via SMTP HELO
  - Senden via Webdav
  - Empfangen via ICQ/Jabber/Skype/...

Transport-Protokolle

- Etwas, mit dem man senden und/oder empfangen kann
- Beliebige Protokolle
  - Empfangen via SMTP HELO
  - Senden via Webdav
  - Empfangen via ICQ/Jabber/Skype/...

Transport-Protokolle

- Etwas, mit dem man senden und/oder empfangen kann
- Beliebige Protokolle
  - Empfangen via SMTP HELO
  - Senden via Webdav
  - Empfangen via ICQ/Jabber/Skype/...

Indirekte Kommunikation

- Wenn ich mit Andre reden will, verschlüssele ich die Nachricht für ihn
- Und füge eine Liste von Empfängern zur Nachricht hinzu
- Jeder der Empfänger kann (nur) die nächste Empfangsadresse sehen
- Andre
  - entschlüsselt die Nachricht,
  - schickt sie weiter, damit niemand weiss, das sie für ihn war

Indirekte Kommunikation

- Wenn ich mit Andre reden will, verschlüssele ich die Nachricht für ihn
- Und füge eine Liste von Empfängern zur Nachricht hinzu
- Jeder der Empfänger kann (nur) die nächste Empfangsadresse sehen
- Andre
  - entschlüsselt die Nachricht,
  - schickt sie weiter, damit niemand weiss, das sie für ihn war

Indirekte Kommunikation

- Wenn ich mit Andre reden will, verschlüssele ich die Nachricht für ihn
- Und füge eine Liste von Empfängern zur Nachricht hinzu
- Jeder der Empfänger kann (nur) die nächste Empfangsadresse sehen
- Andre
  - entschlüsselt die Nachricht,
  - schickt sie weiter, damit niemand weiss, das sie für ihn war

Indirekte Kommunikation

- Wenn ich mit Andre reden will, verschlüssele ich die Nachricht für ihn
- Und füge eine Liste von Empfängern zur Nachricht hinzu
- Jeder der Empfänger kann (nur) die nächste Empfangsadresse sehen
- Andre
  - entschlüsselt die Nachricht,
  - schickt sie weiter, damit niemand weiss, das sie für ihn war

Indirekte Kommunikation

- Wenn ich mit Andre reden will, verschlüssele ich die Nachricht für ihn
- Und füge eine Liste von Empfängern zur Nachricht hinzu
- Jeder der Empfänger kann (nur) die nächste Empfangsadresse sehen
- Andre
  - entschlüsselt die Nachricht,
  - schickt sie weiter, damit niemand weiss, das sie für ihn war

Indirekte Kommunikation

- Wenn ich mit Andre reden will, verschlüssele ich die Nachricht für ihn
- Und füge eine Liste von Empfängern zur Nachricht hinzu
- Jeder der Empfänger kann (nur) die nächste Empfangsadresse sehen
- Andre
  - entschlüsselt die Nachricht,
  - schickt sie weiter, damit niemand weiss, das sie für ihn war

Stand

- Was wurde bereits erledigt
  - Spezifikationen
  - Programme
  - Dokumentation
- Was ist zu tun?
  - Meilensteine

Stand

- Was wurde bereits erledigt
  - Spezifikationen
  - Programme
  - Dokumentation
- Was ist zu tun?
  - Meilensteine

Stand

- Was wurde bereits erledigt
  - Spezifikationen
  - Programme
  - Dokumentation
- Was ist zu tun?
  - Meilensteine

Stand

- Was wurde bereits erledigt
  - Spezifikationen
  - Programme
  - Dokumentation
- Was ist zu tun?
  - Meilensteine

Stand

- Was wurde bereits erledigt
  - Spezifikationen
  - Programme
  - Dokumentation
- Was ist zu tun?
  - Meilensteine

Stand

- Was wurde bereits erledigt
  - Spezifikationen
  - Programme
  - Dokumentation
- Was ist zu tun?
  - Meilensteine

Spezifikationen

- Einige Entwürfe auf https://www.eof.name/projects/eof-1/eof-1/ zu finden
- Wöchentlich neue
- Teilweise schon überarbeitet

Spezifikationen

- Einige Entwürfe auf https://www.eof.name/projects/eof-1/eof-1/ zu finden
- Wöchentlich neue
- Teilweise schon überarbeitet

Spezifikationen

- Einige Entwürfe auf https://www.eof.name/projects/eof-1/eof-1/ zu finden
- Wöchentlich neue
- Teilweise schon überarbeitet

Implementation von EOF-1

- Hauptprogramm ceof zu 20% fertig
- Erste Erfahrungen mit GPGME
- Bibliotheken zu 80% fertig
  - Quelltextsäuberung steht noch an
- Erste GUI fertiggestellt

Implementation von EOF-1

- Hauptprogramm ceof zu 20% fertig
- Erste Erfahrungen mit GPGME
- Bibliotheken zu 80% fertig
  - Quelltextsäuberung steht noch an
- Erste GUI fertiggestellt

Implementation von EOF-1

- Hauptprogramm ceof zu 20% fertig
- Erste Erfahrungen mit GPGME
- Bibliotheken zu 80% fertig
  - Quelltextsäuberung steht noch an
- Erste GUI fertiggestellt

Implementation von EOF-1

- Hauptprogramm ceof zu 20% fertig
- Erste Erfahrungen mit GPGME
- Bibliotheken zu 80% fertig
  - Quelltextsäuberung steht noch an
- Erste GUI fertiggestellt

Implementation von EOF-1

- Hauptprogramm ceof zu 20% fertig
- Erste Erfahrungen mit GPGME
- Bibliotheken zu 80% fertig
  - Quelltextsäuberung steht noch an
- Erste GUI fertiggestellt

Von Dir

- Verwirrt?
- Ist etwas unklar?
- Interessiert?

Von Dir

- Verwirrt?
- Ist etwas unklar?
- Interessiert?

Von Dir

- Verwirrt?
- Ist etwas unklar?
- Interessiert?

Diese Vorstellung

- ...endet hier
- Vielen Dank für die Aufmerksamkeit
- Projektseite: https://www.eof.name/eof-1/
- Kontakt via „telmich (bei) u.eof.name“

Diese Vorstellung

- ...endet hier
- Vielen Dank für die Aufmerksamkeit
- Projektseite: https://www.eof.name/eof-1/
- Kontakt via „telmich (bei) u.eof.name“

Diese Vorstellung

- ...endet hier
- Vielen Dank für die Aufmerksamkeit
- Projektseite: https://www.eof.name/eof-1/
- Kontakt via „telmich (bei) u.eof.name“

Diese Vorstellung

- ...endet hier
- Vielen Dank für die Aufmerksamkeit
- Projektseite: https://www.eof.name/eof-1/
- Kontakt via „telmich (bei) u.eof.name“