IT-Sicherheit Seminar

Remailer: Typ-I bis Typ-III

Mervyn McCreight

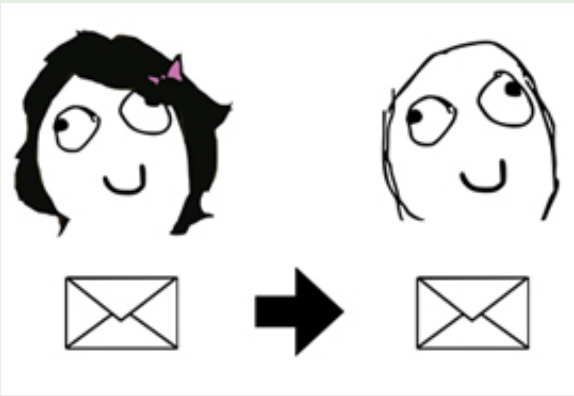
FH-Wedel

2. November 2015

Table of Contents

Warum Remailer?

Sitzung



- Alice möchte Bob Nachricht senden
- Normal: Schutz des Inhalts
- Jetzt: Schutz der Identitäten

Angreifer Eve möchte Ziele gefährden

- Netzwerk beobachten
- Einsicht in Traffic
- Pakete abfangen, senden, manipulieren und senden

Table of Contents

Cypherpunk-Remailer

Wesentliche Eigenschaften

- Klassifizierung: Typ-I Remailer
- "Cipher", "Cyber", "Punk"
- Anonymisierend
- Inspiration: Mix-Netzwerke *(David Chaum)*
- E-Mail Protokoll

Cypherpunk-Remailer

Wesentliche Eigenschaften

- Klassifizierung: Typ-I Remailer
- "Cipher", "Cyber", "Punk"
- Anonymisierend
- Inspiration: Mix-Netzwerke *(David Chaum)*
- E-Mail Protokoll

Cypherpunk-Remailer

Wesentliche Eigenschaften

- Klassifizierung: Typ-I Remailer
- "Cipher", "Cyber", "Punk"
- Anonymisierend
- Inspiration: Mix-Netzwerke *(David Chaum)*
- E-Mail Protokoll

Cypherpunk-Remailer

Wesentliche Eigenschaften

- Klassifizierung: Typ-I Remailer
- "Cipher", "Cyber", "Punk"
- Anonymisierend
- Inspiration: Mix-Netzwerke *(David Chaum)*
- E-Mail Protokoll

Cypherpunk-Remailer

Wesentliche Eigenschaften

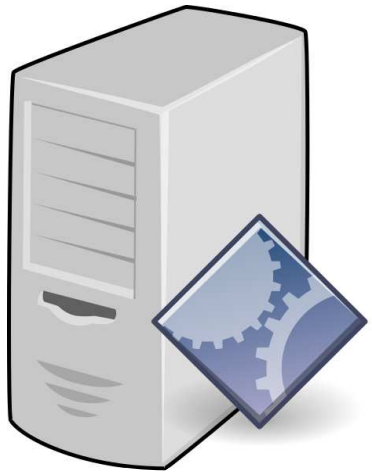
- Klassifizierung: Typ-I Remailer
- "Cipher", "Cyber", "Punk"
- Anonymisierend
- Inspiration: Mix-Netzwerke *(David Chaum)*
- E-Mail Protokoll

Cypherpunk-Remailer

Basis des Protokolls

Netzwerk von mehreren verschiedenen Cypherpunk-Remailern

Cypherpunk-Remailer C



- öffentlicher Schlüssel D_C
- privater Schlüssel E_C
- Nachricht entschlüsseln und weiterleiten
- Nachrichten-Header modifizieren

Cypherpunk-Remailer - Vorbereitung

Alice kennt:

- Remailer-Netzwerk $C_1, C_2, ..., C_n$
- öffentliche Schlüssel $E_{C_1}, E_{C_2}, ..., E_{C_n}$

Alice muss

- Auswahl Remailer
- Reihenfolge bestimmen

Ziel

Nachricht wird über Pfad an Bob gesendet

Cypherpunk-Remailer - Vorbereitung

Inhalt einer Nachricht

- Adresse A
- Nachricht N

schichtenweise Verschlüsselung

$$N' = (A_1, E_{C_1}(A_2, E_{C_2}(...(A_n, E_{C_n}(A_{Bob}, E_{Bob}(N))) \quad (1)$$

Cypherpunk-Remailer - Ablauf

Ablauf Sendevorgang

- Alice sendet N' an C_1
- C_1 erhält A_2 und verschlüsselte Nachricht
- C_1 sendet Nachricht an Adresse in A_2
- C_2 erhält A_3 und verschlüsselte Nachricht
- (...)
- C_n sendet Nachricht an Adresse von Bob

Cypherpunk-Remailer

Was haben wir erreicht?

- C_x kennt nur unmittelbaren Nachfolger und Vorgänger
- Bob kennt nur letzten Remailer
- Alice kennt als Einzige gesamten Pfad

und  ?

Cypherpunk-Remailer - Sicherheitsanalyse

Traffic Analyse

- Nachrichtengröße
- leitet Nachrichten sofort weiter

Replay Angriff

- Eve kann Nachrichten abfangen und wieder einspielen
- Duplikate werden nicht erkannt