
Spam und SPIT

Aktuelle Schutzmöglichkeiten
und Gegenmaßnahmen

Moritz Mertinkat
mmertinkat AT rapidsoft DOT de
06.07.2007

Spam

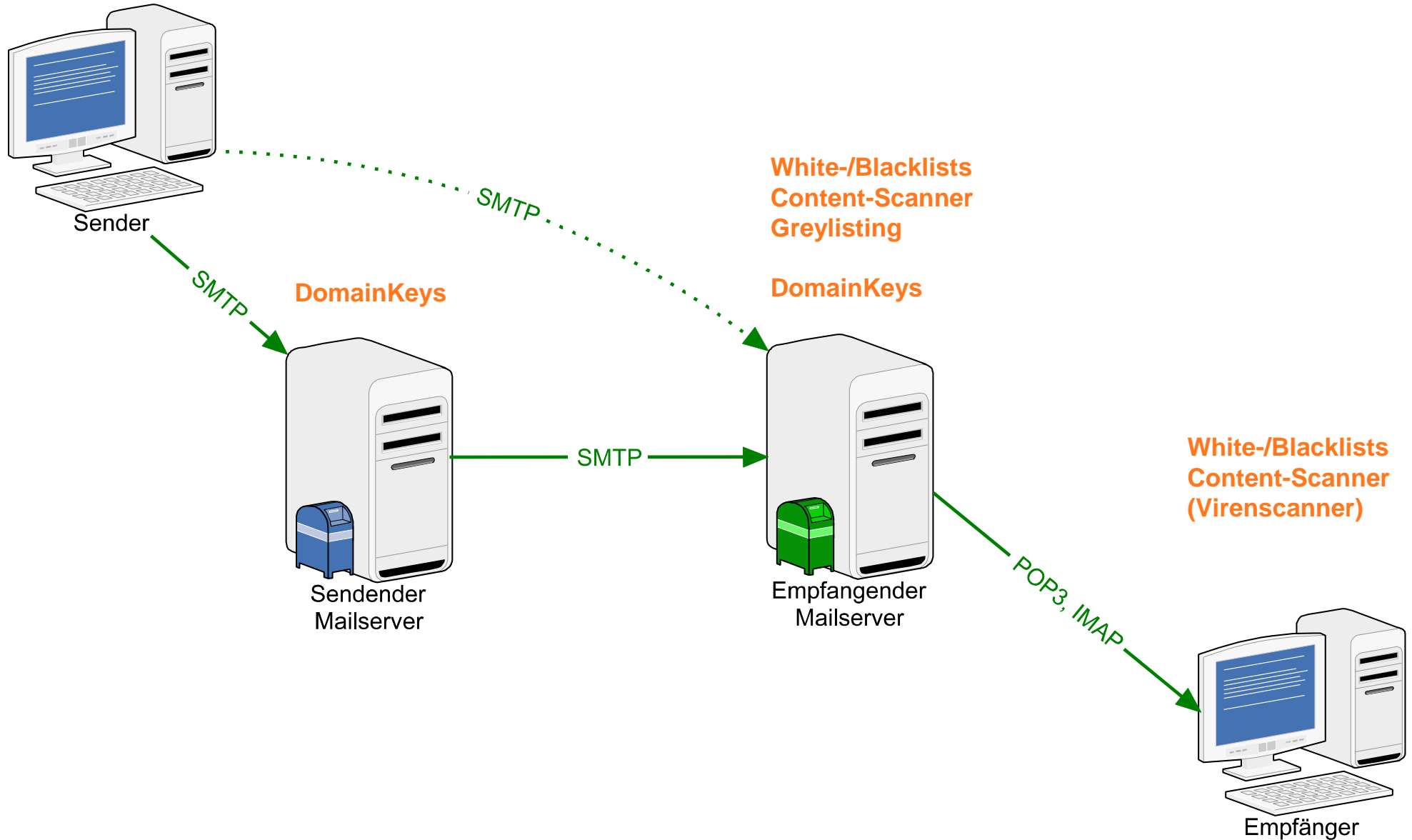
- Architektur
- Schutzmöglichkeiten
- Gegenmaßnahmen

SPIT

- Architektur
- Unterschiede zu Spam
- Schutzmöglichkeiten
- Gegenmaßnahmen

Zusammenfassung
Ausblick

Spam // Architektur

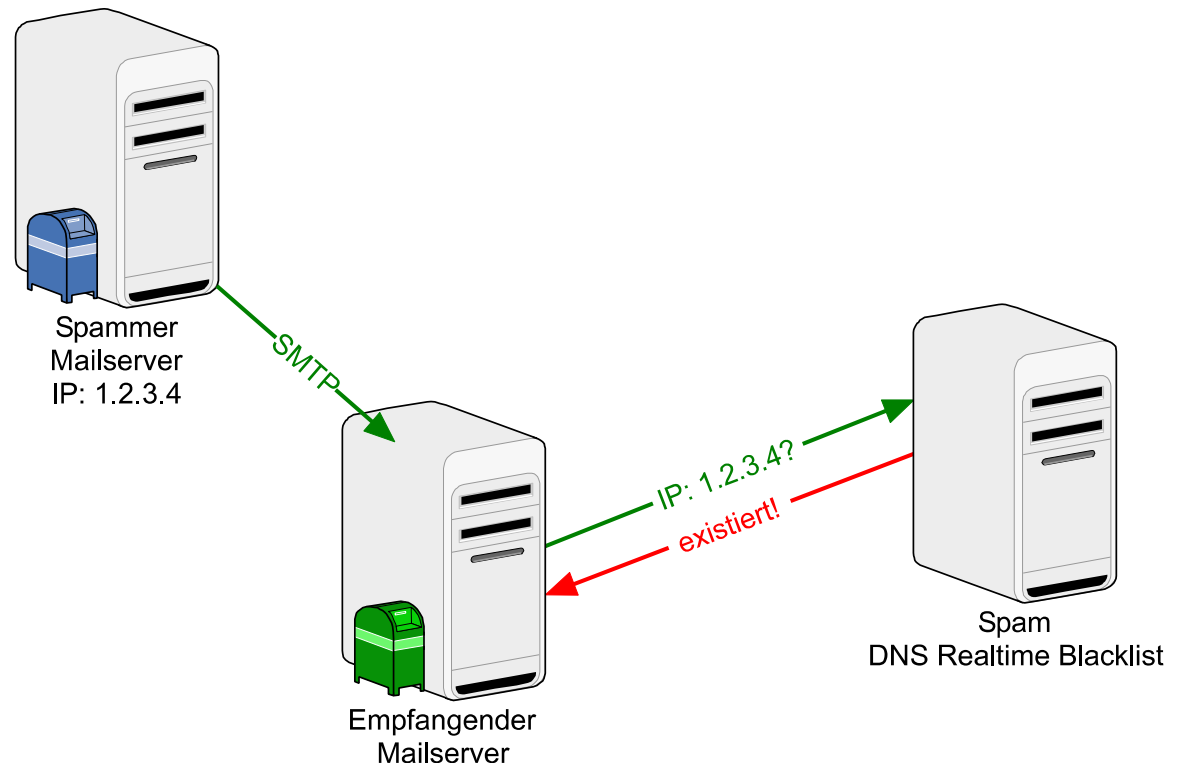


Spam // Schutzmöglichkeiten

DNS Realtime Blacklists

- Blacklisten mit bekannten Spammer-IPs
- Checks über DNS Protokoll in Echtzeit

- Kritisch: "Gute" IP-Adressen in der Liste können zu vielen *false positives* führen



Spam // Schutzmöglichkeiten

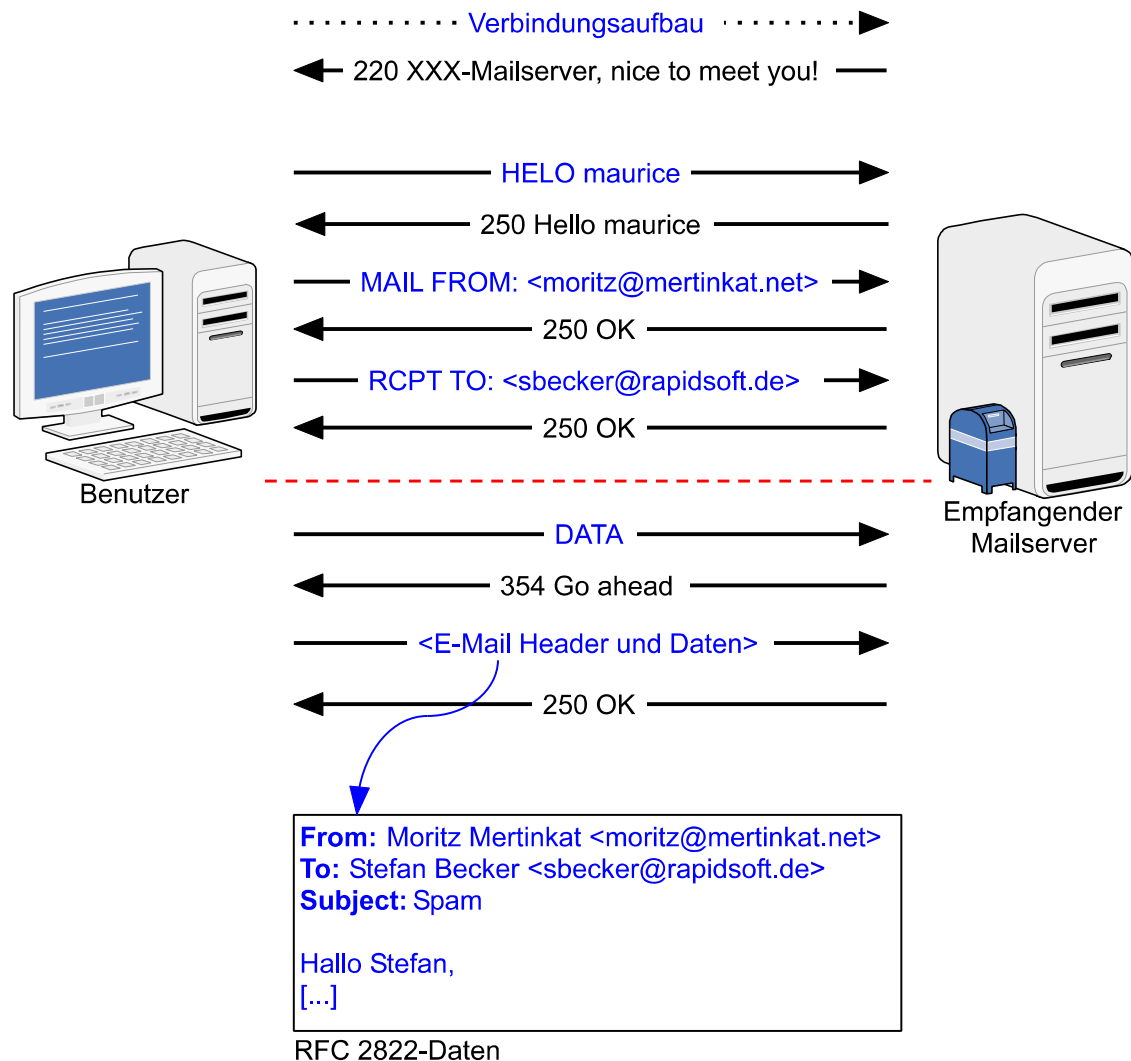
Greylisting 1/4

- Vorgehensweise:
 - Die E-Mail wird mit einem temporären Fehler zurückgewiesen (SMTP Code 4xx)
 - Erst beim zweiten Zustellversuch (mit denselben Identitäten) wird die E-Mail angenommen
- Einsatz nur auf Server sinnvoll
- Software der Spammer unternimmt oft (noch) keinen erneuten Zustellversuch => deutlich weniger Spam

- Greylisting wird bislang noch recht selten eingesetzt (< 1 %)
- Vorteile
 - Deutlich weniger Spam (bis zu 90 %)
 - Automatisches Training der White- und Blacklists
- Nachteile
 - Verzögerung bei der Zustellung
 - Unter Umständen gar keine Zustellung

Spam // Schutzmöglichkeiten

Greylisting 3/4 – SMTP Session



- SMTP-Identitäten sind:
 - IP-Adresse
 - MAIL FROM
 - RCPT TO
- Beim ersten Zustellversuch wird nach RCPT TO abgebrochen

Spam // Schutzmöglichkeiten

Greylisting 4/4

- Einsatz an der UNI Freiburg:

```
220 mailgateway1.uni-freiburg.de ESMTTP I'm pleased to meet you.  
HELO mertinkat.net  
250 mailgateway1.uni-freiburg.de Hello mertinkat.net [xxx.xxx.xxx.xxx]  
MAIL FROM: <moritz@mertinkat.net>  
250 OK  
RCPT TO: <mmertinka@informatik.uni-freiburg.de>  
451-You have been greylisted.  
451 We will accept this mail from you in 15 minutes.  
QUIT  
221 mailgateway1.uni-freiburg.de closing connection
```

- Neue E-Mail Protokolle
 - Extended SMTP (AUTHentication)
 - AMTP (neuer Protokollvorschlag)
(Authenticated Mail Transfer Protocol)

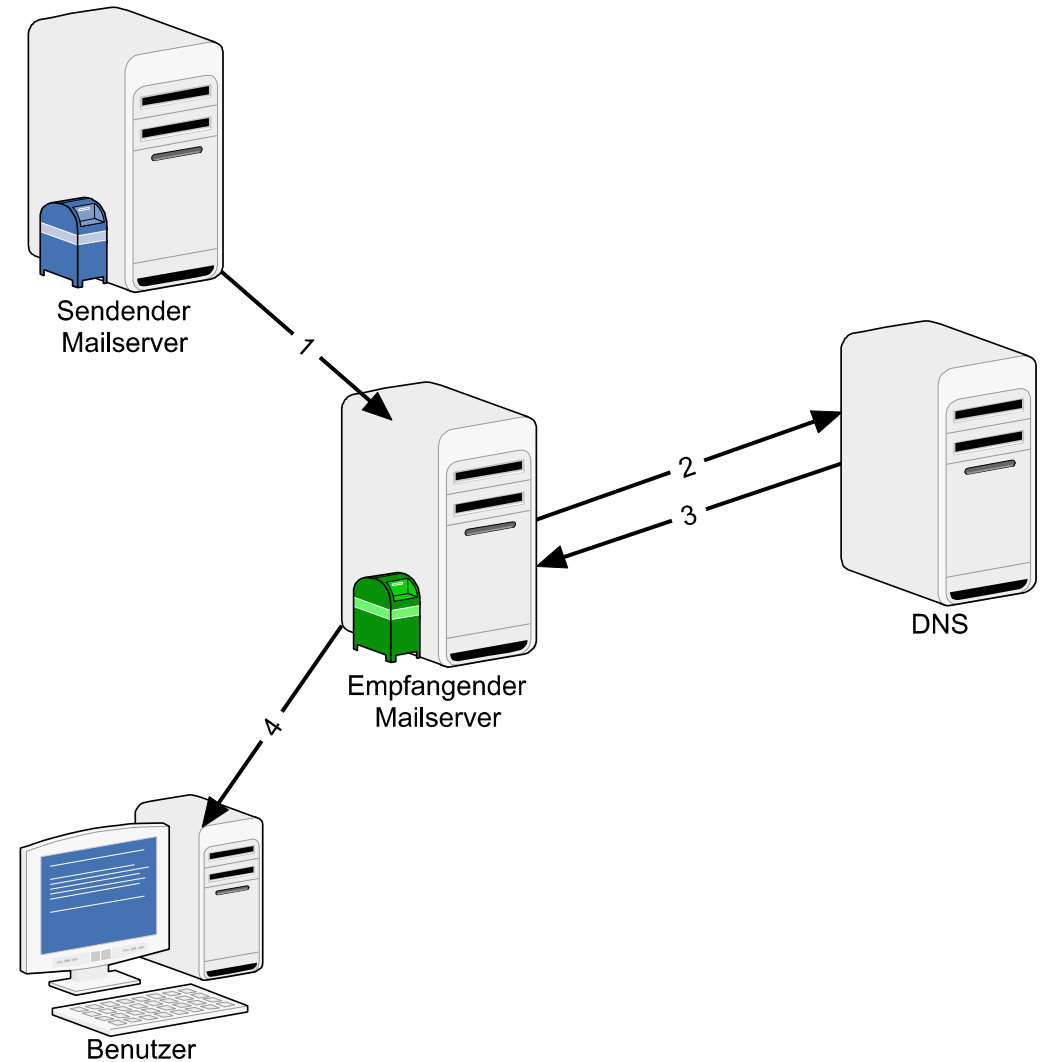
- Signierte E-Mails
 - S/MIME und OpenPGP
 - DKIM (DomainKeys Identified Mail)
 - SPF (Sender Policy Framework)

- DomainKeys Identified Mail
- Vorschlag von Yahoo! zur Vermeidung von Absender-Adressfälschungen
- Kein Mittel, um Spam zu verhindern
- Signierung erfolgt mittels Private und Public Keys
- Nutzt die RFC 2822-Daten (d.h. den Mail-Header), nicht die SMTP-Daten

Spam // Gegenmaßnahmen

DKIM 2/3

- Der sendende Mailserver signiert die E-Mail mit seinem *private key* [1]
- Der *public key* ist im DNS zu seiner Domain hinterlegt
- Der empfangende Mailserver überprüft die Signatur mit dem *public key* aus dem DNS der Absender-Domain [2, 3]
- Wenn die Signatur stimmt, wird die E-Mail zugestellt [4]



- Beispiel einer DKIM-Signatur:

```
DKIM-Signature: v=1; a=rsa-sha256; s=dkim-enabled-mail; d=mertinkat.net;  
c=simple/simple; q=dns/txt;  
h=received:from:to:subject:date:message-id;  
b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB  
4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut  
KVdkLLkpVaVVQPzerDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV  
4bmp/YzhwvcubU4=;
```

```
Received: from mail.mertinkat.net (mail.mertinkat.net [xxx.xxx.xxx.xxx])  
by mail.rapidsoft.de with SMTP; 12 Jun 2007 19:07:55 -0000
```

```
From: Moritz Mertinkat <moritz@mertinkat.net>
```

```
To: Stefan Becker <sbecker@rapidsoft.de>
```

```
Subject: Ist DKIM bereits eingerichtet?
```

```
Date: Tue, 12 Jun 2007 21:07:53 +0200
```

```
Message-ID: <466EEF09.6050508@mertinkat.net>
```

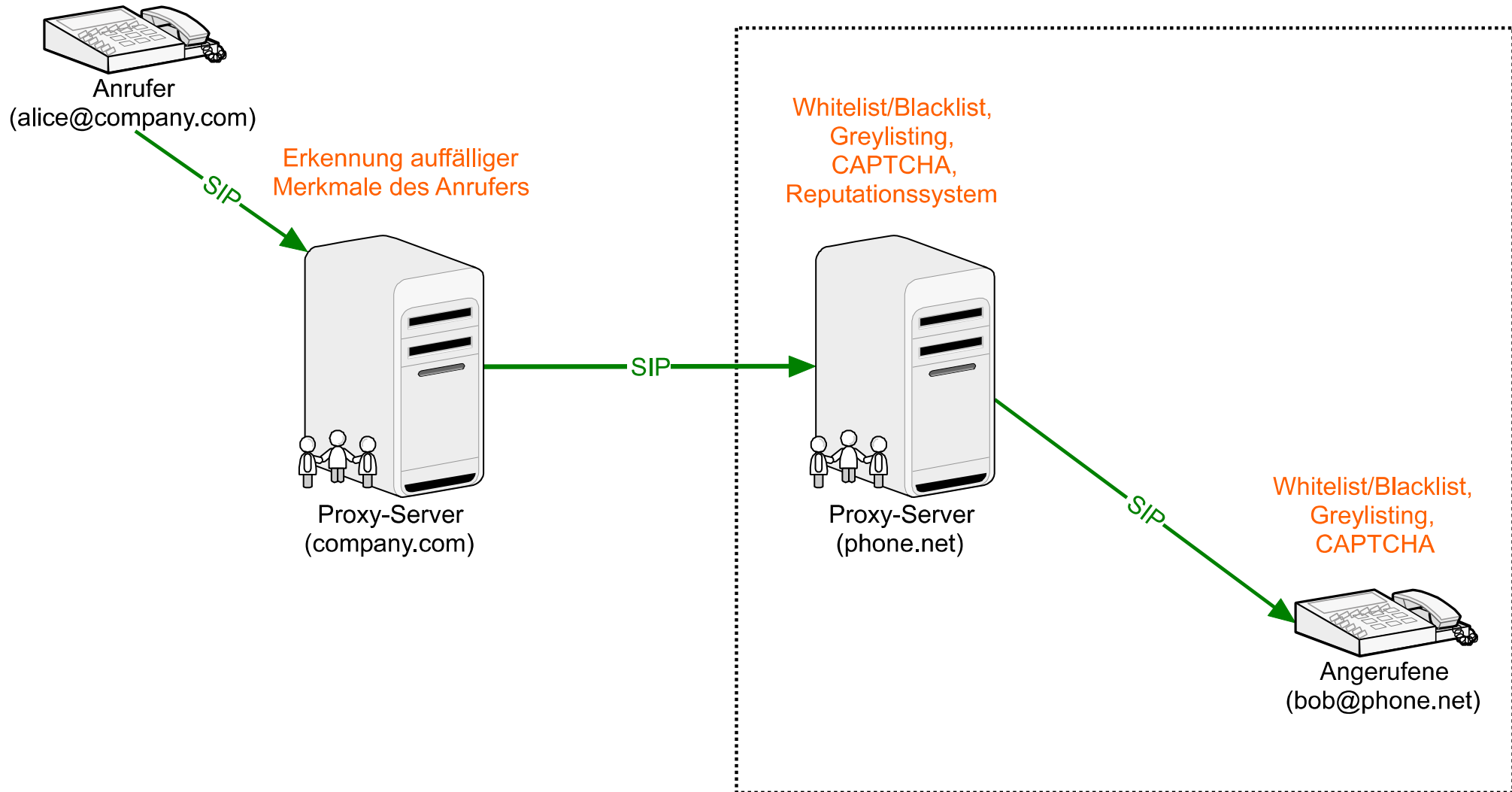
```
Wie ist der Stand?
```

```
Gruß Moritz
```

SPIT // Was ist das?

- SPIT ist *SP*am over *Internet Telephony*
- Werbeanrufe von Call-Centern (oder in Zukunft automatisiert?)
- In Deutschland gesetzlich verboten;
Ausnahmen im gewerblichen Bereich
(BGH-Urteil vom 16.03.1999, Az. XI ZR 76/98)

SPIT // Architektur Internet Telefonie

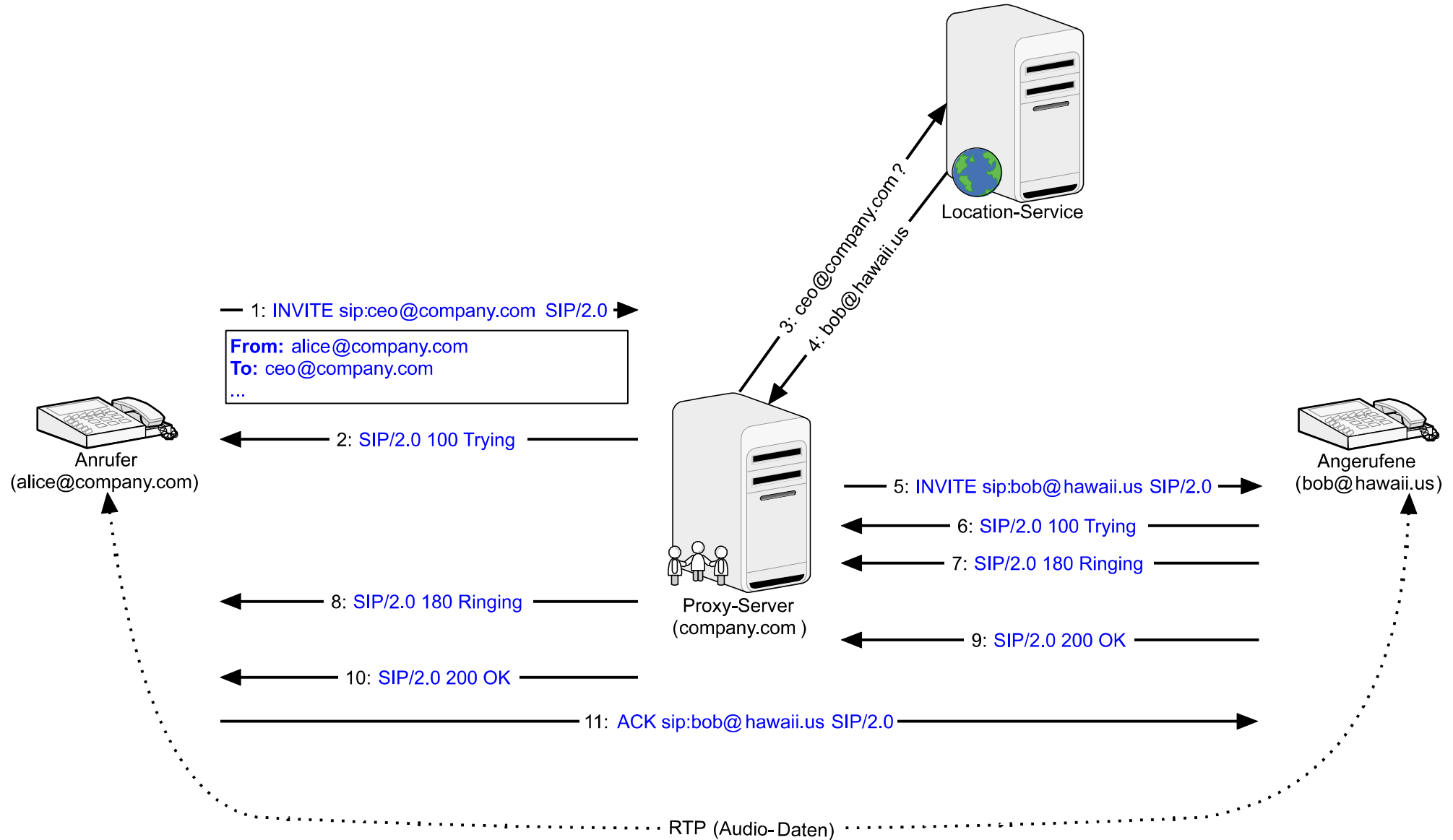


SPIT // Unterschiede zu Spam

- Spam ist asynchron, SPIT synchron
→ die Belästigung tritt *sofort* ein
- **Herausforderung:** Das Telefongespräch muss noch vor dem Klingeln bewertet werden
- → Content-Scanner NICHT möglich
- **Außerdem:** Fernmeldegeheimnis beachten!

SPIT // In geregelten Bahnen

Session Initiation Protocol (SIP)



Zusammenfassung und Ausblick

- Spam ist und wird ein Problem bleiben
- DKIM und Signierung von E-Mails sind aber ein Schritt in die richtige Richtung
- Spammer rüsten ebenfalls nach

- Echter SPIT wird so schnell nicht kommen
 - Spracherkennung noch zu unausgereift
- Weichenstellung aber trotzdem JETZT wichtig

Vielen Dank fürs Zuhören!

Bei Fragen stehe ich gerne
zur Verfügung.

Moritz Mertinkat
mmertinkat AT rapidsoft DOT de