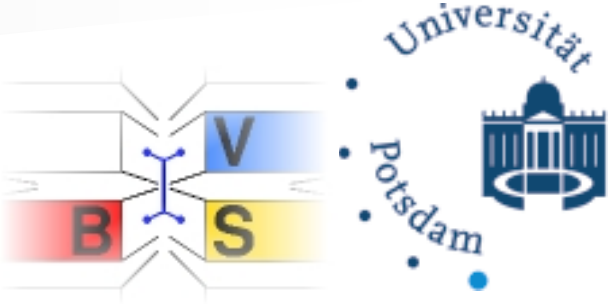
Vermeidung von SPAM-Anrufen in der IP-Telefonie

Stefan Liske, Klaus Rebensburg, Bettina Schnor
Universität Potsdam, Institut für Informatik

9. ENUM-Tag der DENIC
3. September 2007



http://www.cs.uni-potsdam.de

Universität Potsdam, Institut für Informatik

- Institut für Informatik

  ≈ 800 Studenten

- Universität Potsdam
  - gegr. 1991
  - 5 Fakultäten

Agenda

- Motivation
- SIP-Anruf & SPIT

- SPIT-Erkennung
- SPIT-Bekanntgabe
- SPIT-Abwehr
- SPIT-Abwehr $\Rightarrow$ SPIT-Erkennung

- Fazit & Ausblick

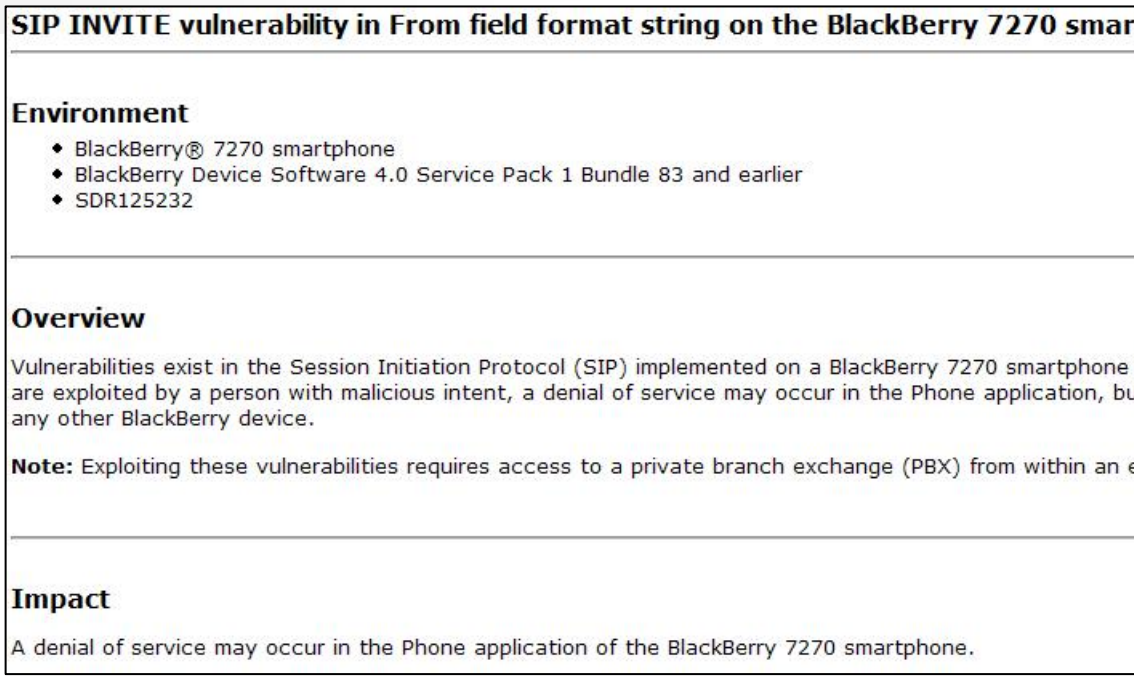
Motivation: SPAM

- Werbung
- Phishing
- Pharming
- Viren
- Trojaner
- Würmer
- ...

⇒ Missbrauch der E-Mail-Infrastruktur

Motivation: SPIT

- Werbung
- Phishing
- Pharming
- Viren
- Trojaner
- Würmer
- ...



SIP INVITE vulnerability in From field format string on the BlackBerry 7270 smar

Environment

- BlackBerry® 7270 smartphone
- BlackBerry Device Software 4.0 Service Pack 1 Bundle 83 and earlier
- SDR125232

Overview

Vulnerabilities exist in the Session Initiation Protocol (SIP) implemented on a BlackBerry 7270 smartphone
are exploited by a person with malicious intent, a denial of service may occur in the Phone application, bu
any other BlackBerry device.

Note: Exploiting these vulnerabilities requires access to a private branch exchange (PBX) from within an e

Impact

A denial of service may occur in the Phone application of the BlackBerry 7270 smartphone.

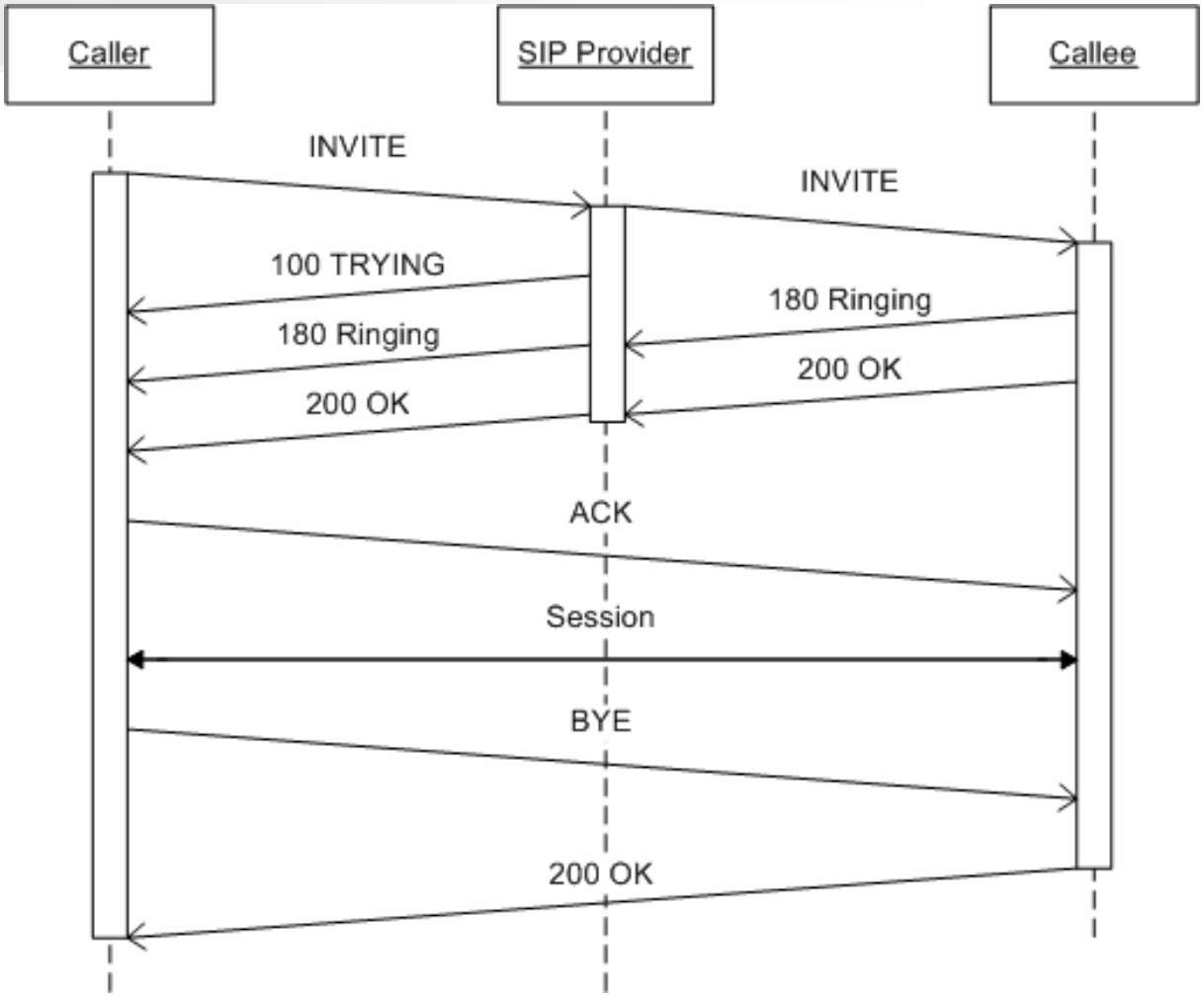
⇒ Missbrauch der VoIP-Infrastruktur

Motivation: Gründe für SPIT

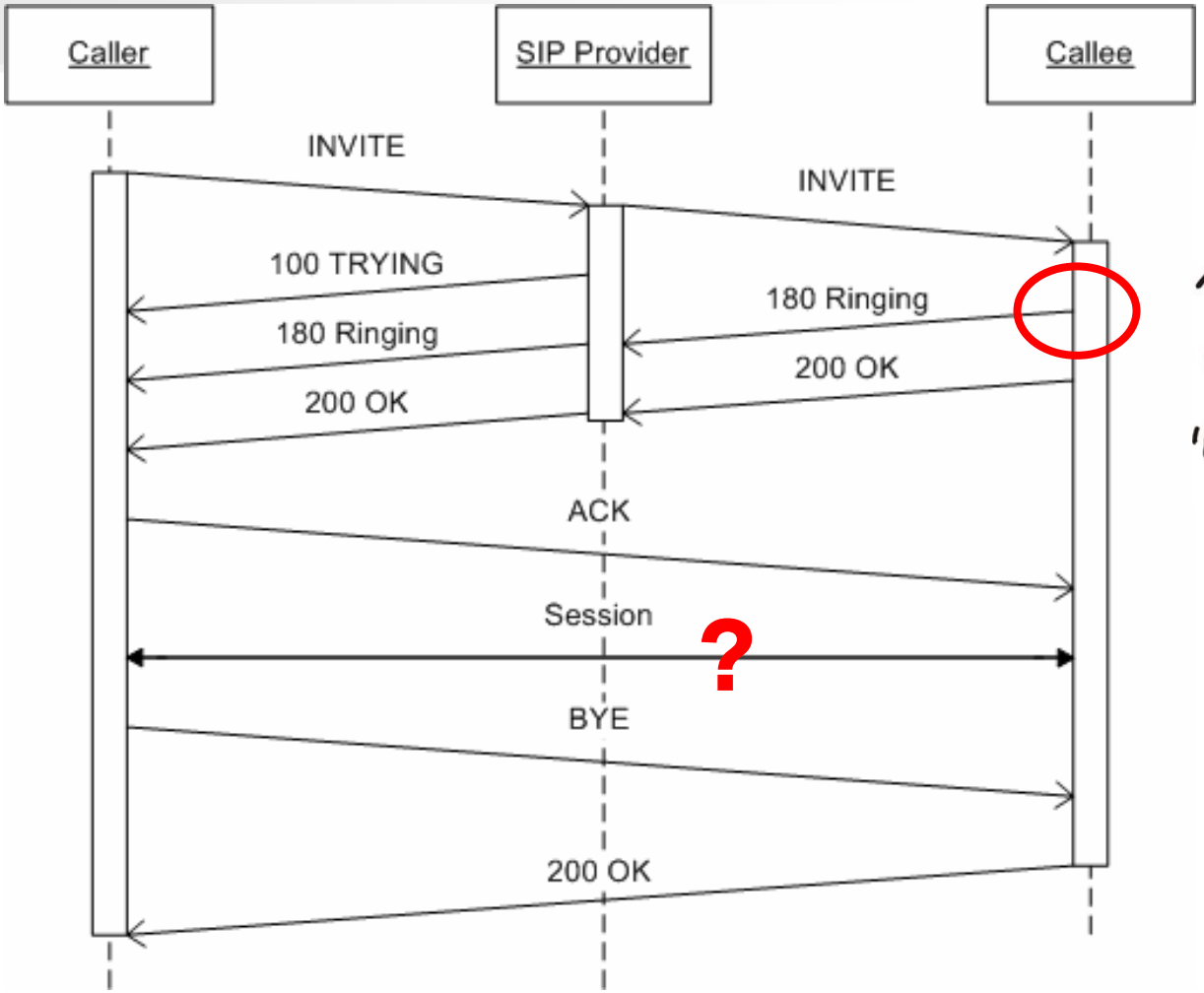
- Zugrundeliegendes IP-Netzwerk
- Verschleierung des Anrufers
- Geringere Kosten

- Geld verdienen
- Fremdes Geld ausgeben

Einfacher SIP-Anruf



Ab wann stört SPIT?



SPIT-Erkennung

- Nicht praktikabel sind
  - Vorgeschaltete Voice-Boxen
  - Nennen alternativer Rufnummern
  - Content-Analyse, -Filter
  - Turing-Tests
  - Computational Puzzles
  - Social Networks, Circle of Trust, Distributed White-Lists
  - Eigenmächties, providerseitiges Unterdrücken von Gesprächen

SPIT-Erkennung

- Analyse der INVITE-Nachricht

```
INVITE sip:user2@sip.uni-potsdam.de SIP/2.0
Call-ID: e6b9aaa79d1e488aeeaed3bd3482614b@141.89.59.49
CSeq: 1 INVITE
From: <sip:user1@sip.uni-potsdam.de>;tag=124cd3c4
To: <sip:user2@sip.uni-potsdam.de>
Via: SIP/2.0/UDP sip.uni-potsdam.de:5060;branch=z9hG4bKx8s…z7t
Via: SIP/2.0/UDP 141.89.59.49:5060;branch=z9hG4bK933…049
Max-Forwards: 70
Subject: Are you awake, yet?
Contact: <sip:141.89.59.49:5060>
Content-Length: 142

(SDP content not shown)
```

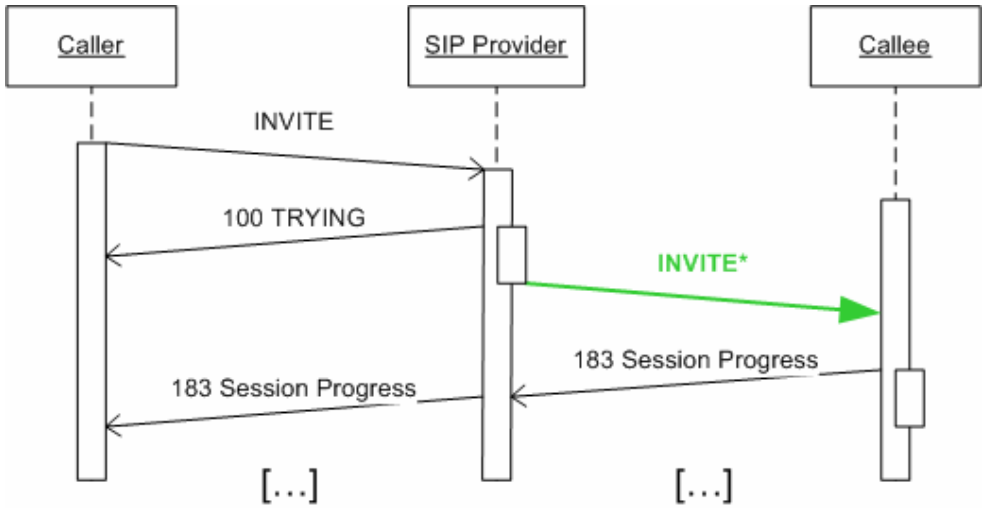
- Analyse des Zeitpunktes

SPIT-Erkennung

- Black-, White-Listen
- Rückrufbeziehungen
- Analyse des Telefonieverhaltens
  - Fehlgewählte Anrufe
  - Gleichzeitige Gespräche
  - Durchschnittliche Gesprächsdauer
  - Anzahl der kontaktierten Personen
  - Anzahl geführter Telefonate
  - Einseitiges Beenden der Gespräche
  - Zeitpunkte vorheriger Anrufe
- Reputationssysteme
- VoIP-Infrastruktur
  - Anrufer identifizieren
  - Anrufer authentifizieren
  - Providervermittelte Gespräche
  - Gegenseitiges Authentifizieren der Provider zueinander
  - Verbindlichkeit der Nachrichten für einen Gesprächsaufbau

SPIT-Bekanntgabe

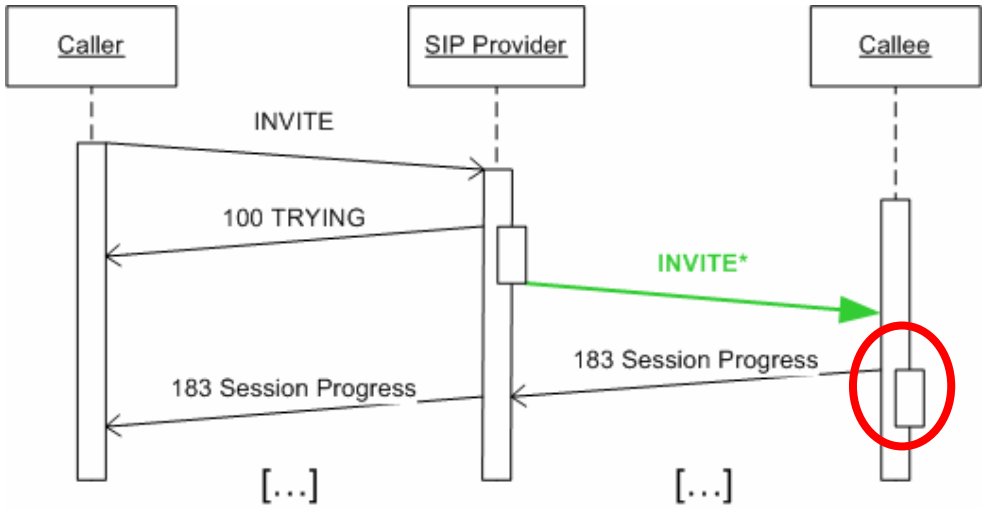
```
INVITE sip:user2@sip.uni-potsdam.de SIP/2.0
Call-ID: e6b9aaa79d1e488aeeaed3bd3482614b@141.89.59.49
CSeq: 1 INVITE
From: <sip:user1@sip.uni-potsdam.de>;tag=124cd3c4
To: <sip:user2@sip.uni-potsdam.de>
Via: SIP/2.0/UDP sip.uni-potsdam.de:5060;branch=z9hG4bKx8s…z7t
Via: SIP/2.0/UDP 141.89.59.49:5060;branch=z9hG4bK933…049
Spitclass: proxy=2; rating=0.03
Max-Forwards: 69
Subject: Are you awake, yet?
Contact: <sip:141.89.59.49:5060>
Content-Length: 142

(SDP content not shown)
```



SPIT-Abwehr

- SPIT-Einschätzung berechnen
  - SPIT-Kalkulationen der Provider benutzen
  - Eigene Module initiieren
  - Gesamteinschätzung berechnen

- Reaktion auf eingehenden Anruf
  - Sofortiges Signalisieren
  - Gebührenanforderung
  - Sofortiges Ablehnen

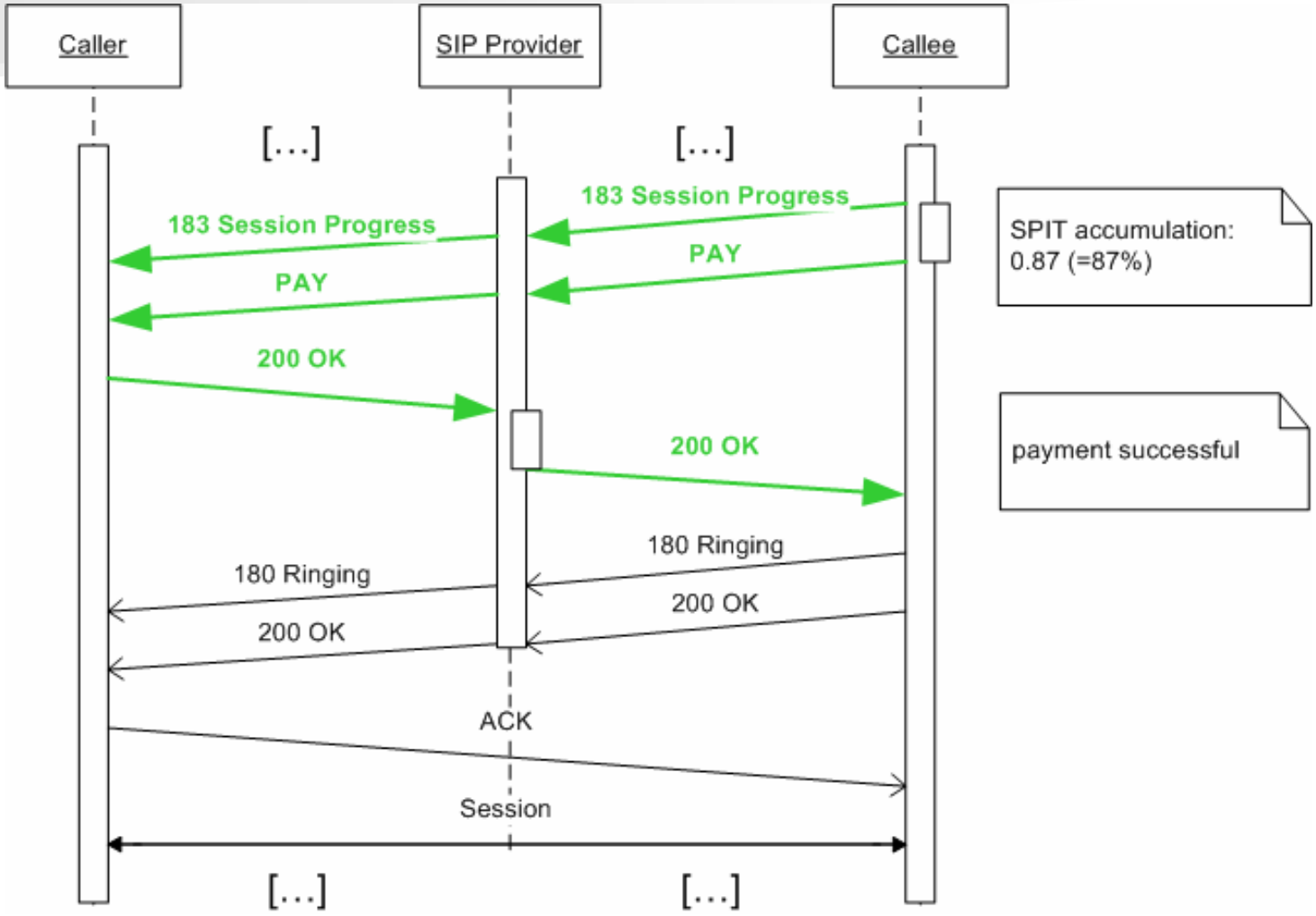


SPIT-Abwehr: Gebührenanforderung

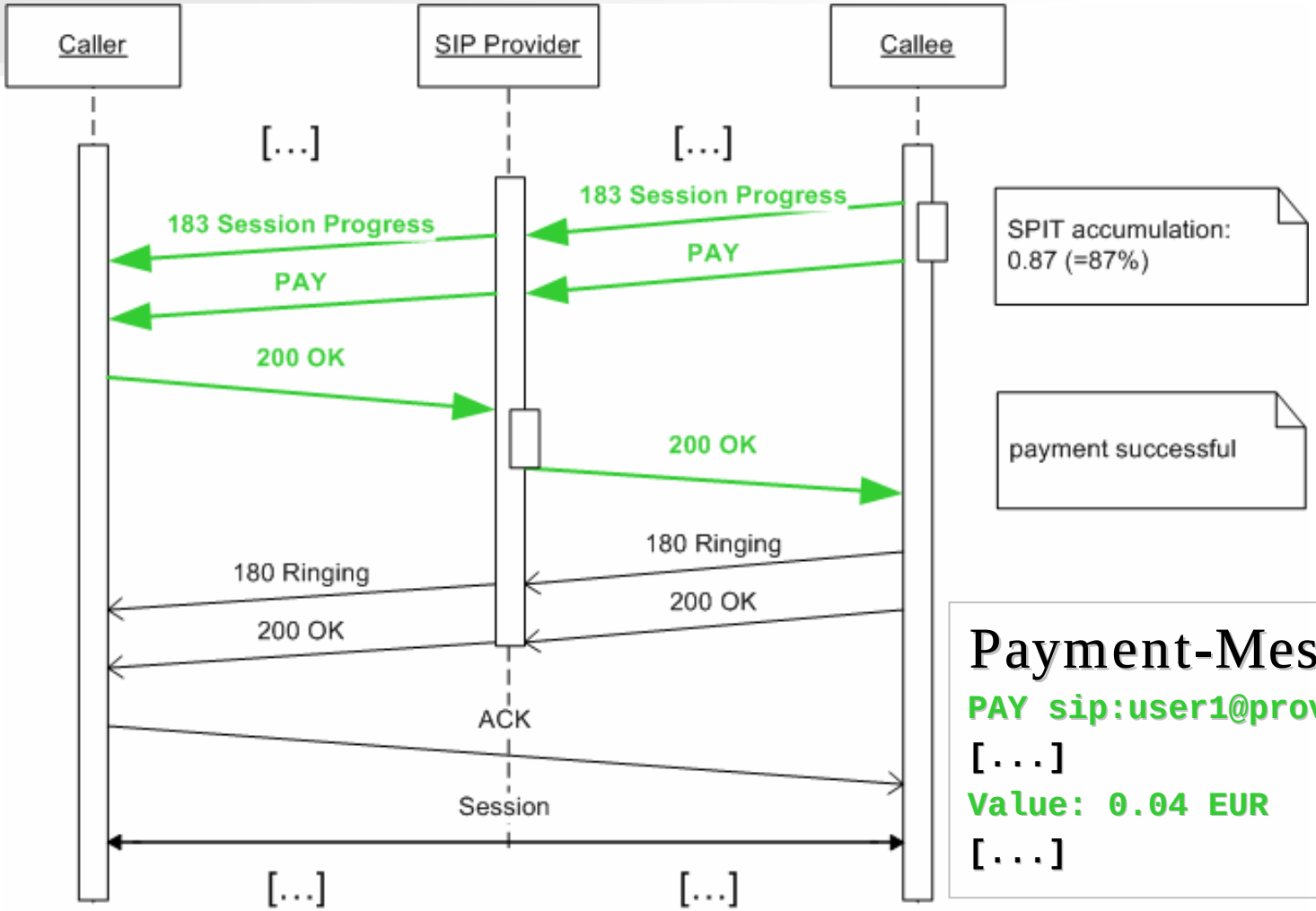
- Payment for Services in Session Initiation Protocol
  - IETF Internet-Draft, C. Jennings (et al.), Juli 2007
  - Transaktion geringer Beträge, Initialkosten/Zeit-Vorauszahlung, außenstehender Bezahlprovider, SIP-Erweiterung um SAML-Nachrichten, Rückerstattung ungeklärt

- Integrated Payment to prevent SPIT
  - Proceedings of KiVS – NetSec 2007, Workshop „Secure Network Configuration“
  - Transaktion geringer Beträge, Initialkosten, integrierter Bezahldienst, SIP-Erweiterung um Request, Transaktionen korrespondieren zum SIP-Dialog

SPIT-Abwehr: Gebührenanforderung



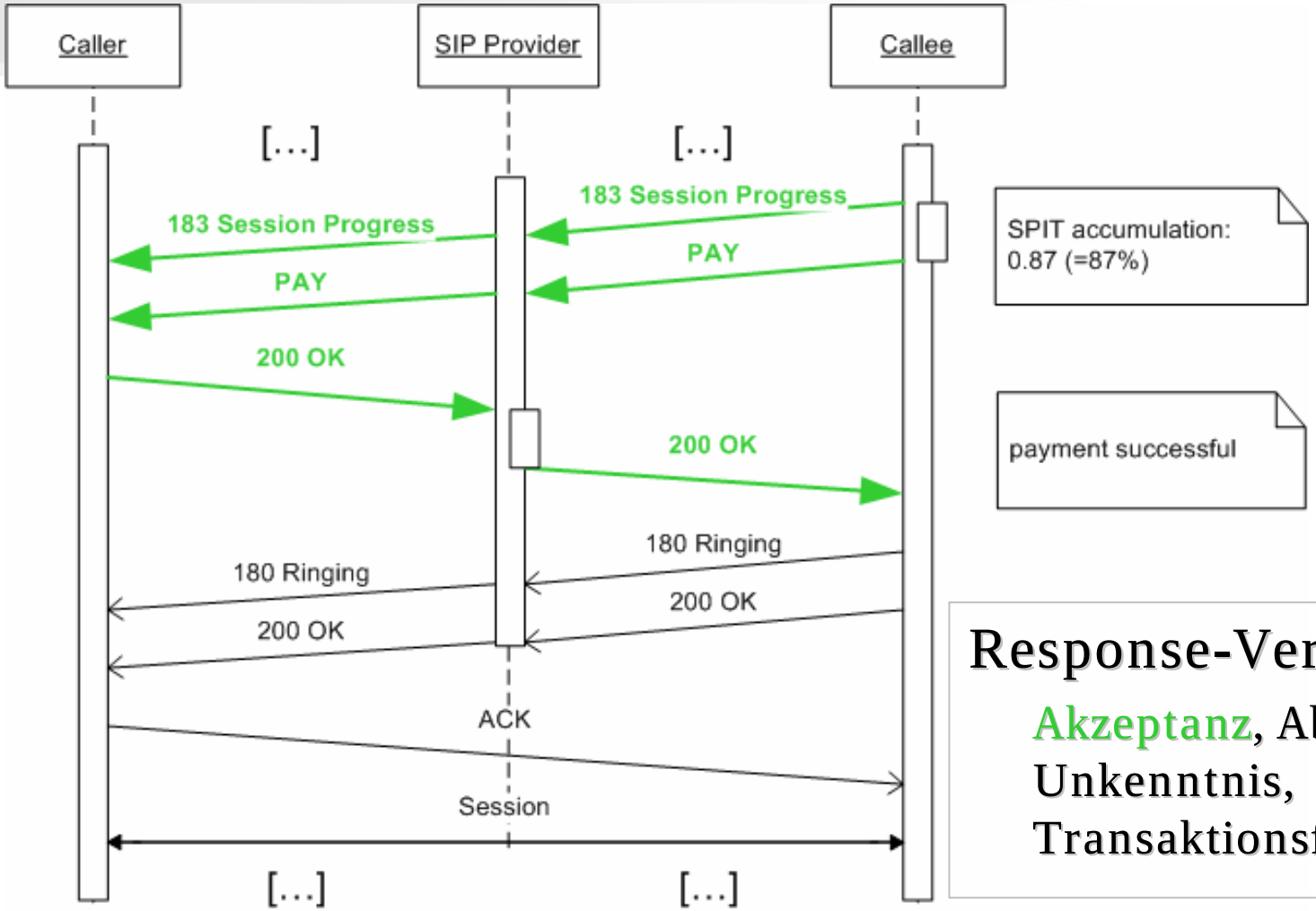
SPIT-Abwehr: Gebührenanforderung



Payment-Message

```
PAY sip:user1@provider.de SIP/2.0
[...]
Value: 0.04 EUR
[...]
```

SPIT-Abwehr: Gebührenanforderung



Response-Verhalten

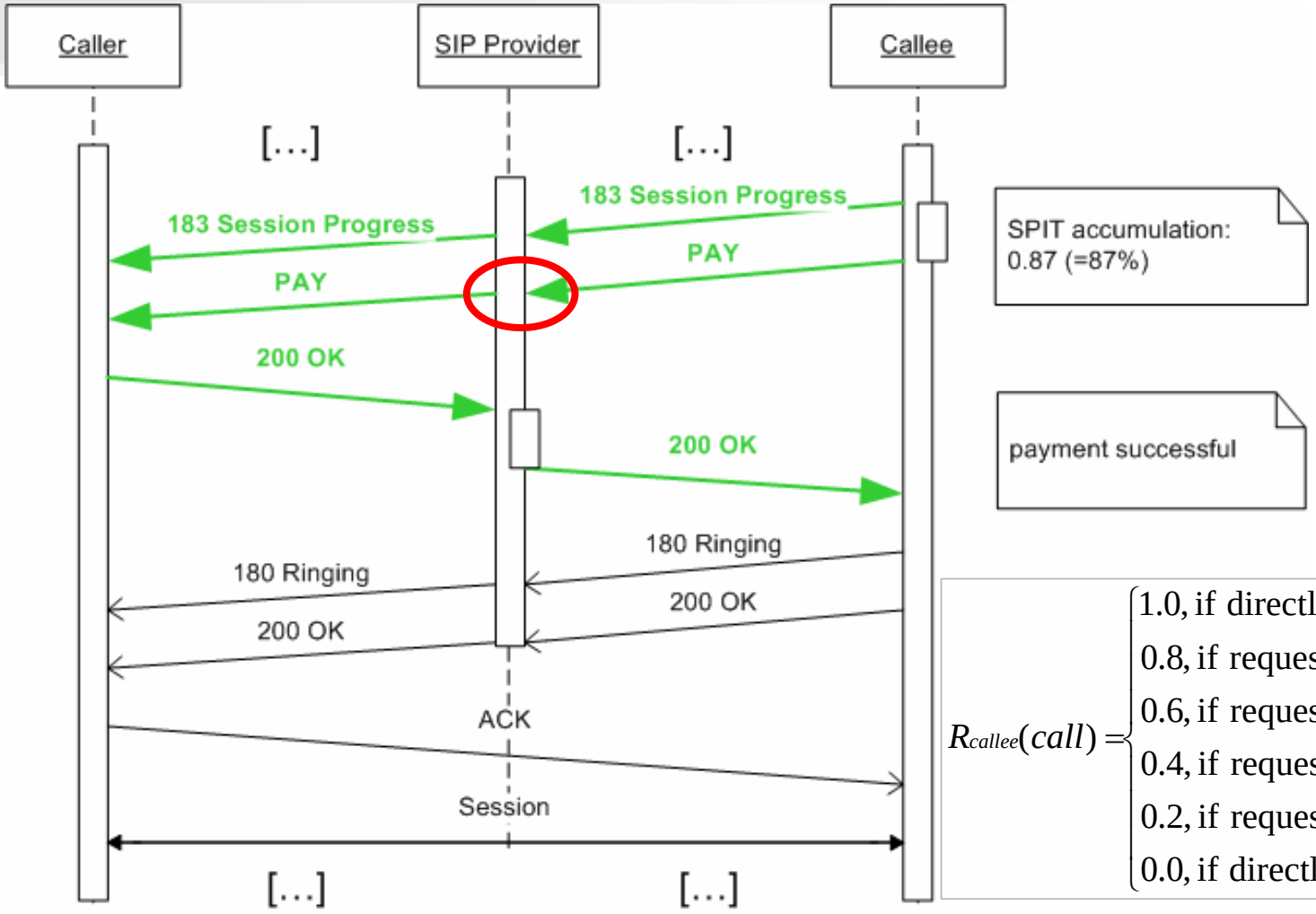
Akzeptanz, Ablehnung, Unkenntnis, Transaktionsfehler

SPIT-Abwehr ⇒ SPIT-Erkennung

- Gebühren...
- ...zur Abwehr vom SPIT
- VoIP-Provider sieht und versteht (Bezahl-) Nachrichten bis zum Beginn des Gesprächs

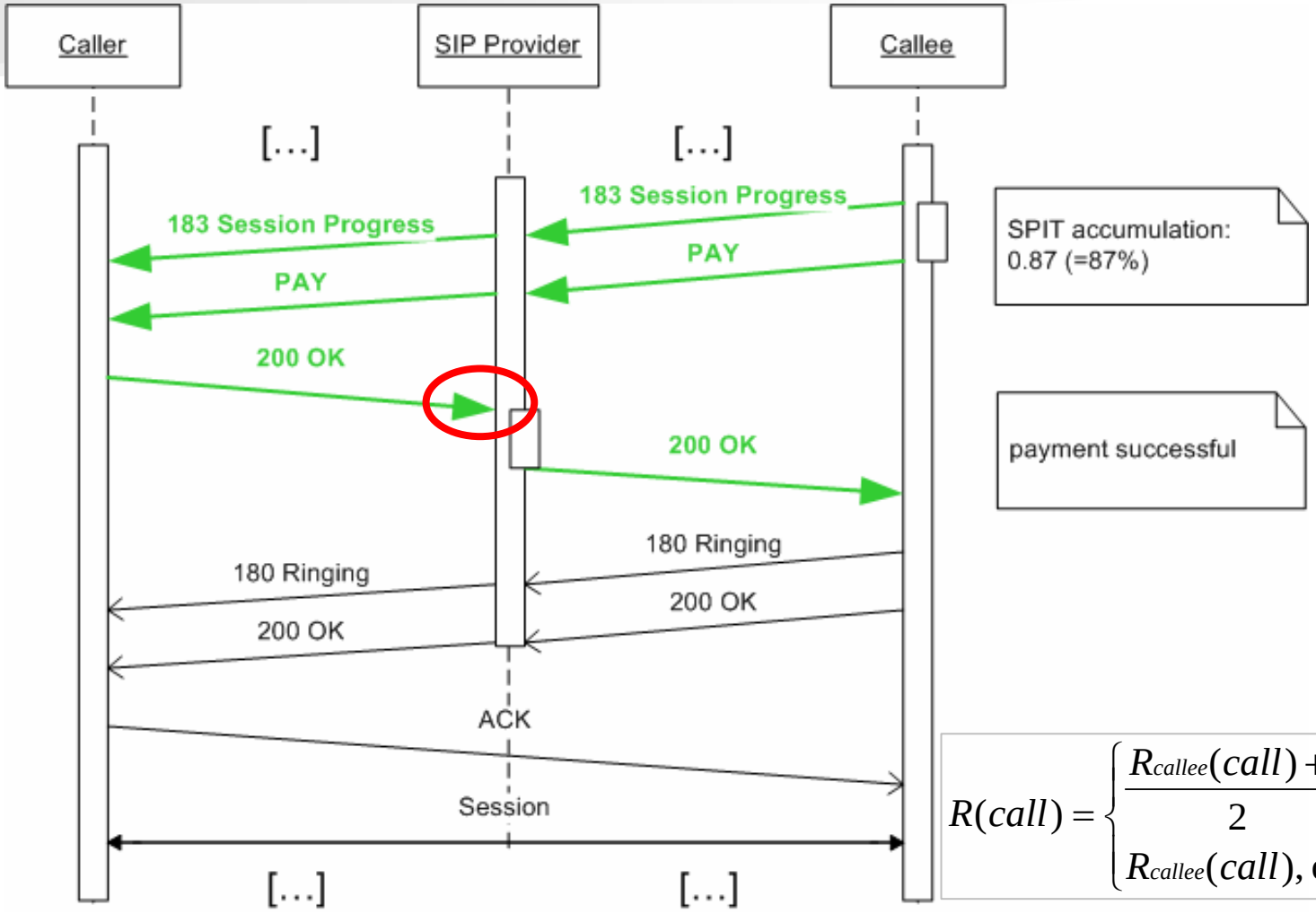
⇒ Implizites Reputationssystem

SPIT-Erkennung: Implizite Reputation



$$R_{callee}(call) = \begin{cases} 1.0, \text{if directly responding 180 or 200} \\ 0.8, \text{if requested 0.01 EUR fee} \\ 0.6, \text{if requested 0.02 EUR fee} \\ 0.4, \text{if requested 0.03 EUR fee} \\ 0.2, \text{if requested 0.04 EUR fee} \\ 0.0, \text{if directly responding 403} \end{cases}$$

SPIT-Erkennung: Implizite Reputation

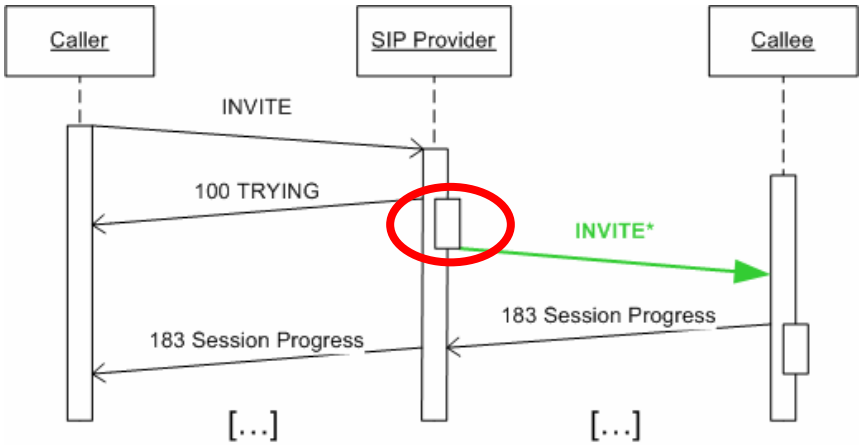


$$R(call) = \begin{cases} \frac{R_{callee}(call)+1}{2}, \text{if accepting a fee} \\ R_{callee}(call), \text{otherwise} \end{cases}$$

SPIT-Erkennung: Implizite Reputation

- Kalkulation einer Gesamtreputation, welche in die Prognose zukünftiger Anrufe einfließt
  - Berechnung der Reputation aus Sicht der einzelnen Angerufenen

$$R_{u2u}(u_o, u_d) = \frac{\sum_{c \in rated(u_o, u_d)} R(c)}{|rated(u_o, u_d)|}$$



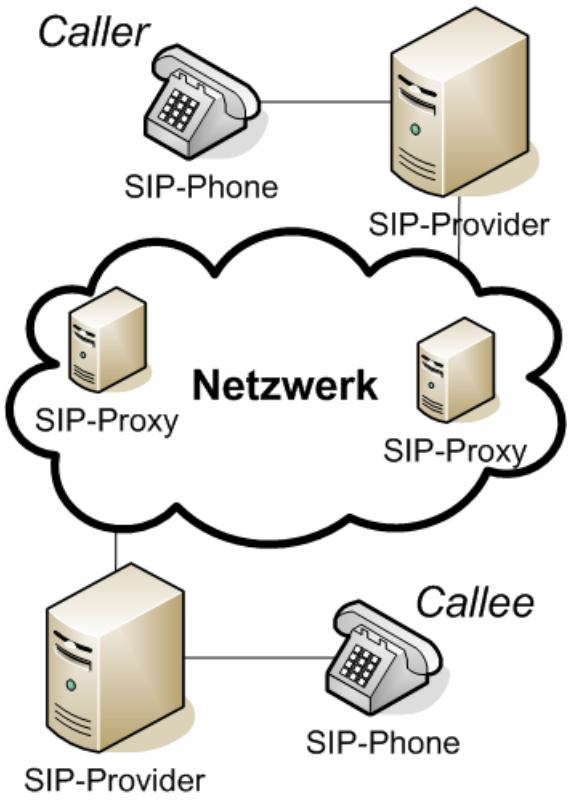
  - Gesamtberechnung

$$R_u(u_o) = \frac{\sum_{u_d \in called(u_o)} R_{u2u}(u_o, u_d)}{|called(u_o, u_d)|}$$

Fazit & Ausblick

- Modulare SPIT-Analyse
- SPITCLASS-Header für SPIT-Bekanntgabe
- PAY-Message (& Response-Verhalten) als Abwehrmaßnahme
- In-The-Middle-Micropayment
- Implizite Reputation
- Anonymität erlaubt

- Keine direkten Gespräche möglich



- Wirkungsgrad, Laufzeitverhalten der einzelnen Module testen

- Verbindlichkeit von SIP-Nachrichten

- Interaktion der Bezahldienste

- Standardisieren unserer Ansätze