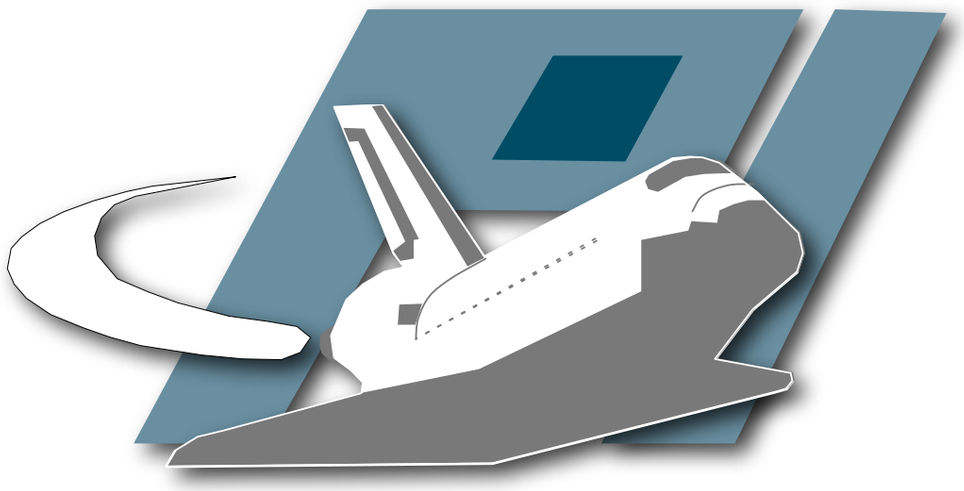
TrumanBox - Transparente Emulation von Internetdiensten

15. DFN Workshop

Christian Gorecki



Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITÄT MANNHEIM

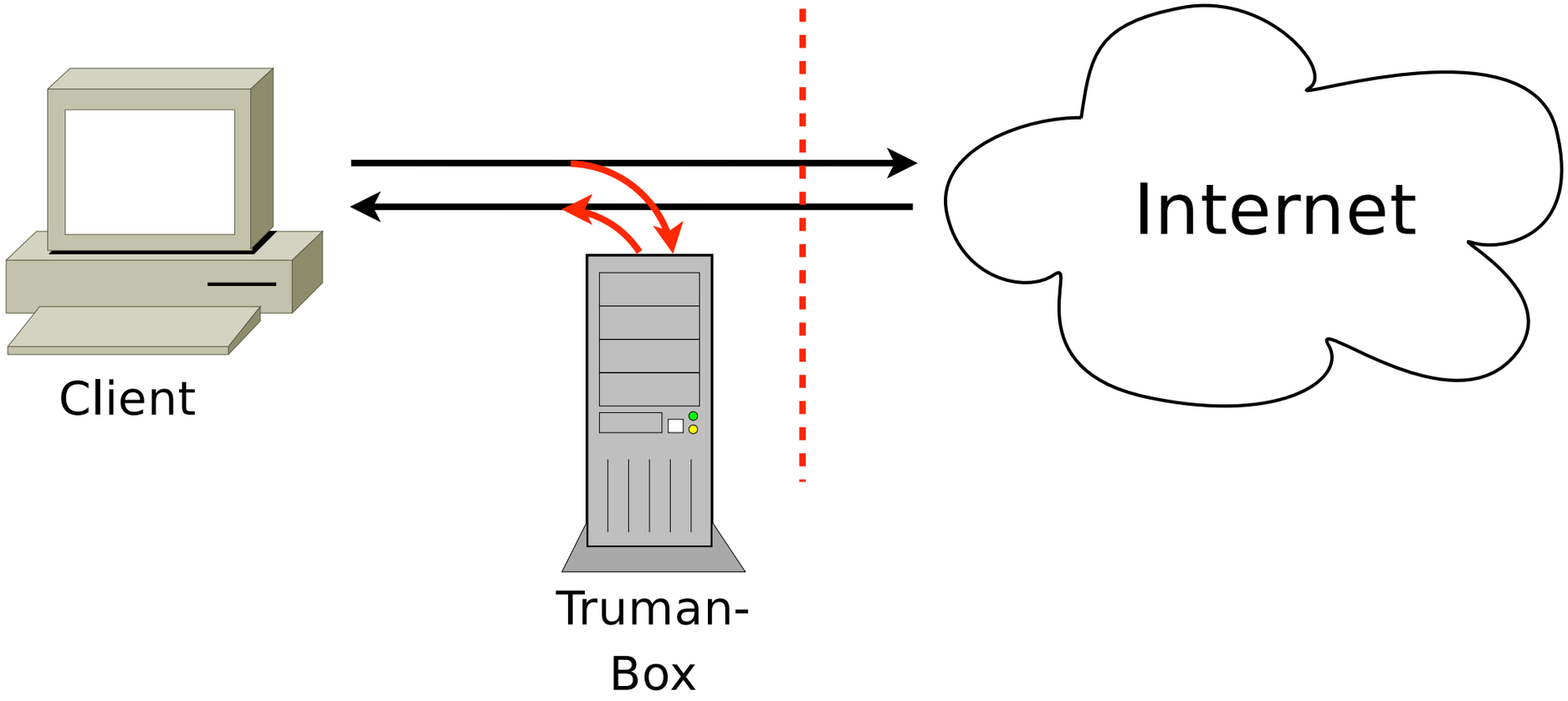
TrumanBox

- Hintergrund
  - Es gibt Honeypots / Honeynets und Honeywall
  - Wünschenswert:
    - Voller Zugriff auf das Internet, ohne das Risiko eine dritte Partei zu infizieren

    ⇒ Emulation als Ausweg

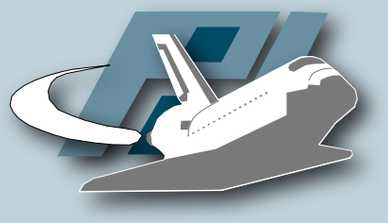
Emulation

- Es muss kein vollständiger Zugriff erlaubt werden
- Der Client muss nur denken, dass Zugriff möglich ist ⇒ *Emulation*



Transparenz

- Bridging anstatt Routing
  - Transparenter Proxy
    - Manipulation der Kommunikation
      - Platzierung der TrumanBox flexibel
- Unabhängig von Malware-Analyse-Plattform
  - CWSandbox und andere Plattformen möglich



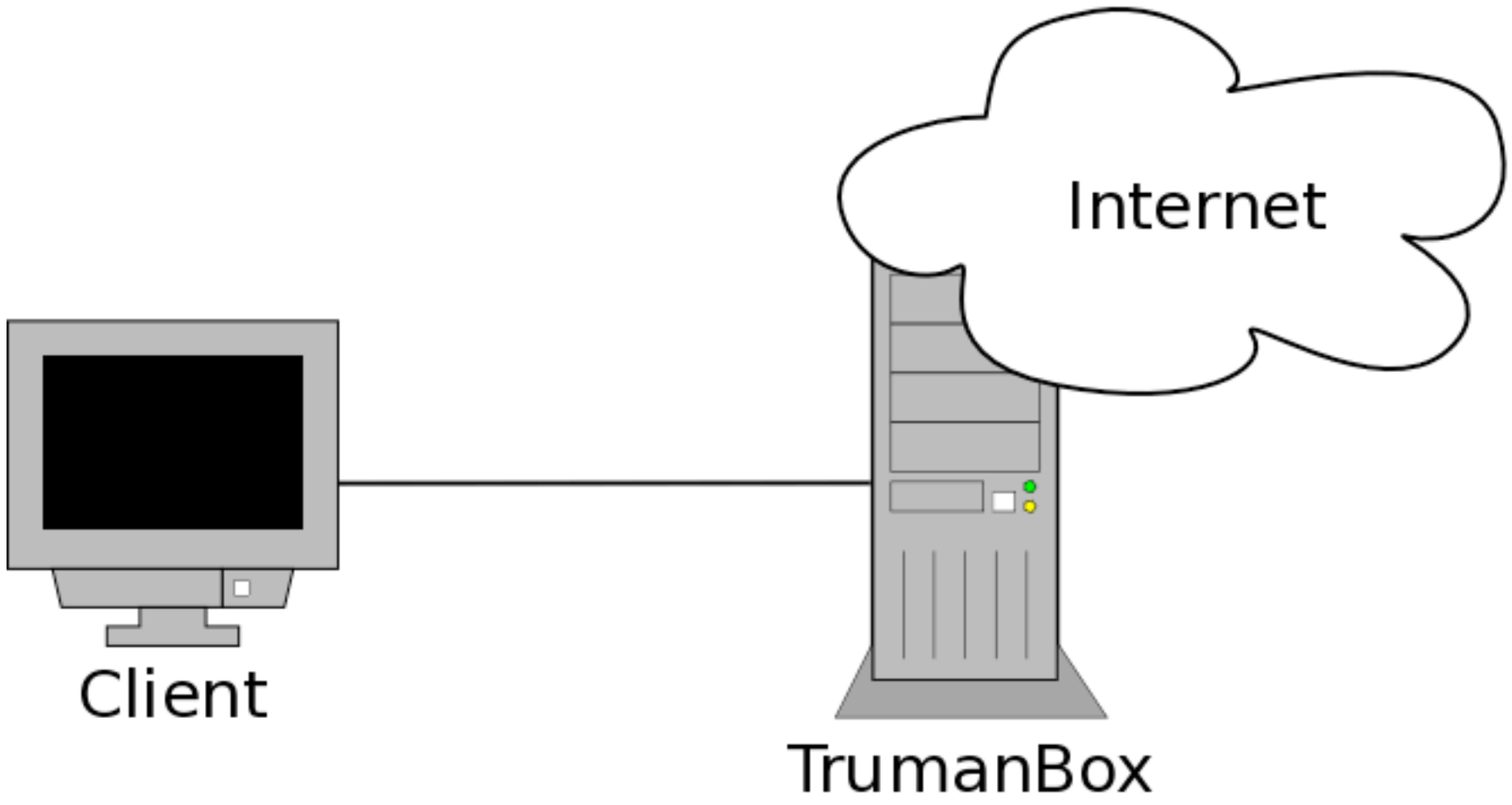
Generisches Verhalten

- Generische Dienste
  - Es wird zur Verfügung gestellt, was angefragt wird
    - Dynamisches Dateisystem
    - Zugriff mit beliebigem Passwort
    - Original-Banner einspielen
  - Jedes unterstützte Protokoll wird auf allen Netzwerkports angeboten
    - HTTP auf TCP Port 5711 und FTP auf 80

Status: Modi

- *Emulation*: Dispatching zu lokalem Dienst
- *Half-Proxy*: Dispatching zu lokalem Dienst und Zusatzinformation von Original-Server
- *Full-Proxy*: Dispatching zu Original-Server und Inhalts-Filterung
- *Transparent*: Kein Dispatching, nur zum Logging und Beobachten
- *One-Box-Emulation:* Dienste werden auf einem Rechner auf einem Interface bereitgestellt

One-Box-Emulation



Status: Protokolle

- TCP
  - HTTP
  - FTP (passive)
  - SMTP
  - IRC
- ICMP
- UDP

ICMP & UDP

- ICMP Pakete werden tranzparent auf TrumanBox umgelenkt
- UDP
  - Per Default keine Antwort

    ⇒ Echo-Responder

Analyseergebnisse

- Mit TrumanBox oft gleiche oder "bessere Ergebnisse" als ohne
- Manchmal schlechtere Ergebnisse:
  - Kein aktives FTP
  - Fehlende Authentifizierung im SMTP
  - Zufall
- (Fast) kein Unterschied zwischen Halb-Proxy und Emulations Modus

Bessere Ergebnisse?

- Oft sind Server nicht mehr online
- Ohne TrumanBox:
  - Entsprechende Funktionen werden nicht geschaltet
- Mit TrumanBox:
  - Interaktion ist dennoch geboten

Ausgewählte Bsp. I

```
1    <winsock_section>
2     <connections_unknown>
3       <connection connectionestablished="0" socket="0" >
4         <gethostbyname requested_host="new.najd.us"
5 resulting_addr="63.173.172.98" />
6       </connection>
7     </connections_unknown>
8     <connections_outgoing>
9       <connection protocol="IRC" connectionestablished="1" socket="352"
10 transportprotocol="TCP" remoteaddr="63.173.172.98" remoteport="51115" >
11          <irc_data nick="gm-784361508" non_rfc_conform="0" servername="0"
12 username="mbhvhefgz" realname="gm-784361508" hostname="0" >
13            <channel password="dcpass" name="#dc" />
14            <notice_deleted value=":irc.localhost NOTICE gm-784361508 :Server is
15 currently in split-mode." />
16          </irc_data>
17        </connection>
18      </connections_outgoing>
19    </winsock_section>
```

remoteport="51115"
nick="gm-784361508"
username="mbhvhefgz"
channel password="dcpass"
channel name="#dc"

Ausgewählte Bsp. II

```
1
2     <icmp_section>
3       <ping request_size="33" host="60.213.176.195" />
4       <ping request_size="33" host="60.213.1
5       <ping request_size="33" host="60.213.9
6       <ping request_size="33" host="60.213.1
7       <ping request_size="33" host="60.213.36.54" />
8       <ping request_size="33" host="60.213.15.128" />
9
        .
10      .    [snip 882 ICMP echo requests]
11
12      <ping request_size="33" host="60.213.242.232" />
13      <ping request_size="33" host="60.213.126.242" />
14      <ping request_size="33" host="60.213.41.213" />
15    </icmp_section>
16
17    <winsock_section>
18      <connections_unknown>
19        <connection connectionestablished="0" socket="0" />
20      </connections_unknown>
21      <connections_outgoing_blocked>
22        <connection connectionestablished="0" socket="1404"
23  transportprotocol="TCP" remoteaddr="60.213.176.195" remoteport="139" />
24        <connection connectionestablished="0" socket="1
25  transportprotocol="TCP" remoteaddr="60.213.176.195" rem
26        <connection connectionestablished="0" socket="1
27  transportprotocol="TCP" remoteaddr="60.213.106.254" rem
28        <connection connectionestablished="0" socket="1
29  transportprotocol="TCP" remoteaddr="60.213.106.254" rem
30        <connection connectionestablished="0" socket="1460"
31  transportprotocol="TCP" remoteaddr="60.213.99.31" remoteport="139" />
32        <connection connectionestablished="0" socket="1460"
33  transportprotocol="TCP" remoteaddr="60.213.99.31" remoteport="445" />
34        <connection connectionestablished="0" socket="1464"
35  transportprotocol="TCP" remoteaddr="60.213.144.65" remoteport="139" />
36        <connection connectionestablished="0" socket="1464"
37  transportprotocol="TCP" remoteaddr="60.213.144.65" remoteport="445" />
38        <connection connectionestablished="0" socket="1468"
39  transportprotocol="TCP" remoteaddr="60.213.36.54" remoteport="139" />
40        <connection connectionestablished="0" socket="1468"
41  transportprotocol="TCP" remoteaddr="60.213.36.54" remoteport="445" />
42      </connections_outgoing_blocked>
43    </winsock_section>
```

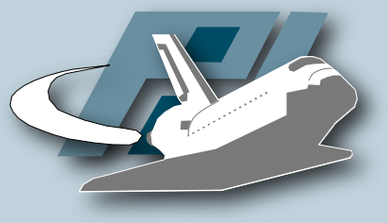
ping request_size="33 host="60.213.176.195"

transportprotocol="TCP" remoteaddr= "60.213.176.195" remoteport="139"

Ausgewählte Bsp. III

```
24        <connection protocol="HTTP" connectionestablished="1" socket="1740"
25  transportprotocol="TCP" remoteaddr="207.46.225.221" remoteport="80" >
26          <http_data>
27            <http_cmd method="GET" url="/" http_version="HTTP/1.0" >
28              <header_data>
29                <header>Host: windowsupdate.microsoft.com</header>
30                <header>Pragma: no-cache</header>
31              </header_data>
32            </http_cmd>
33          </http_data>
34        </connection>
35        <connection protocol="IRC" connectionestablished="1" socket="1776"
36  transportprotocol="TCP" remoteaddr="208.185.80.120" remoteport="6511" >
37          <irc_data password="goahead" nick="[P00|DEU|21
38  servername="0" username="XP-3563" realname="ADMIN-8DCF
39            <channel password="norockeds" name="#matrix"
40            <notice_deleted value=":irc.localhost NOTICE
41  is currently in split-mode." />
42          </irc_data>
43        </connection>
44        <connection protocol="HTTP" connectionestablishe
45  transportprotocol="TCP" remoteaddr="61.121.100.107" re
46          <http_data>
47            <http_cmd method="GET" url="/mute/c/prxjdg.cgi"
48  http_version="HTTP/1.0" >
49              <header_data>
50                <header>Host: hpcgi1.nifty.com</header>
51                <header>Pragma: no-cache</header>
52              </header_data>
53            </http_cmd>
```

password="goahead"
nick="[P00|DEU|21482]"
username="XP-3563"
channel password="norockeds"
channel name="#matrix"



TrumanBox & VMware

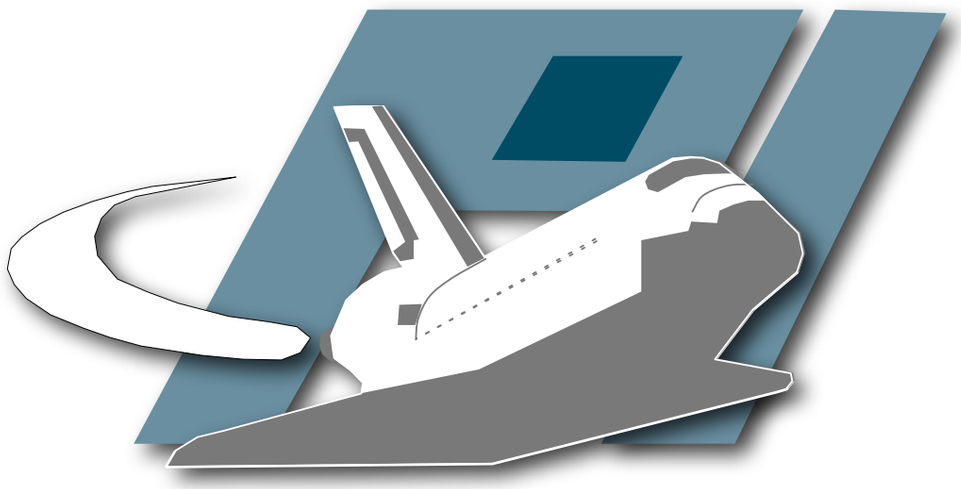
- TrumanBox unter VMware nicht stabil
  - Weder auf Windows, noch auf Linux Host
  - Grund: Bridging innerhalb eines virtuellen Netzwerkes

⇒ TrumanBox auf nativem System

Christian Gorecki
http://pi1.informatik.uni-mannheim.de/
gorecki@informatik.uni-mannheim.de

Fragen?

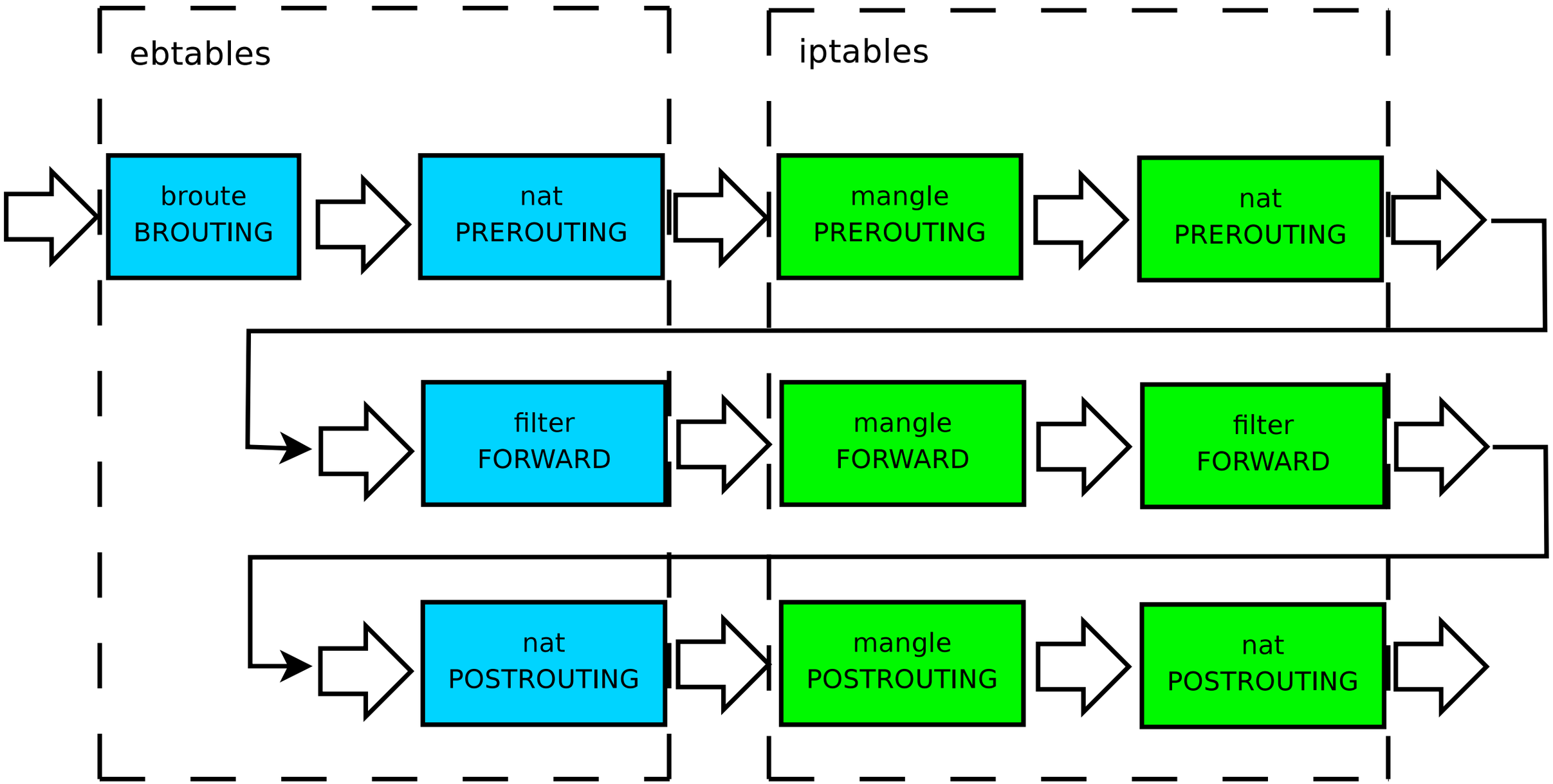
Danke für Ihre Aufmerksamkeit!



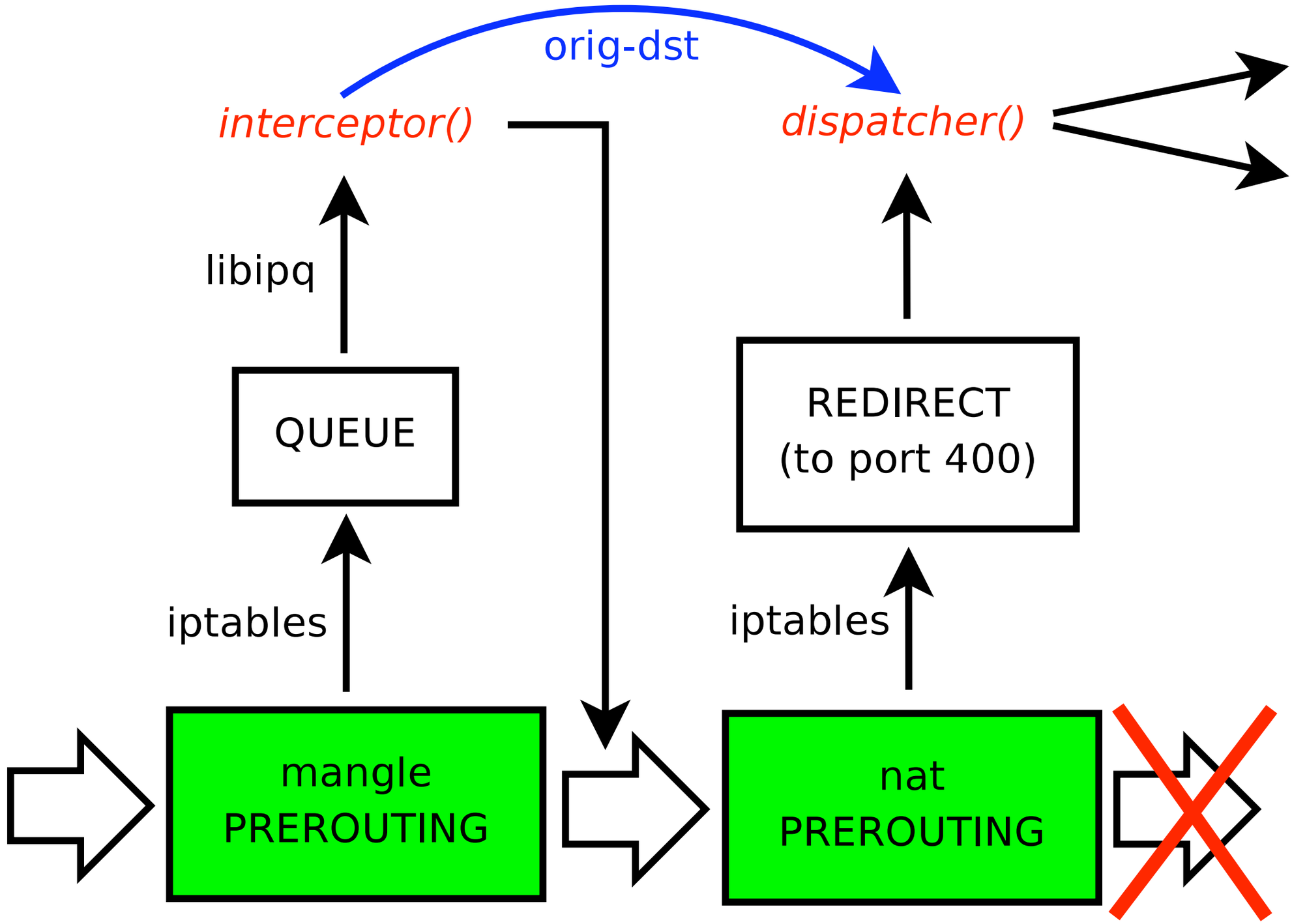
Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITÄT MANNHEIM

Paketfluß innerhalb einer Bridge



Redirecting



System Struktur