ICMP Protokoll & Anwendung

Einige Risiken von ICMP erkennen und verstehen !

FRITZ Gerald

- Betrachtungen auf Protokollebene
  - ICMP, Begriffsdefinition, warum/wozu
  - ICMP Message Types
  - ICMP TYPE Field
  - ICMP Error
- ICMP Host Detection auf Basis von ICMP
  - Broadcast ICMP
  - Inverse Mapping
- Passive fingerprinting, eine Einführung
  - einige Vorteile
  - Architektur

Betrachtungen auf Protokollebene

Grau, teurer Freund, ist alle Theorie . . .

- ICMP $\Rightarrow$ **I**nternet **C**ontrol **M**essage **P**rotokoll
- . . . die zwei Hauptgründe warum ICMP:
  - Router und/oder Zielrechner informieren den Sender über Fehler im Umgang mit IP-Packeten.
  - Testen der Netzwerkverbindung und Ermittlung allgemeiner Daten über die Eigenschaften der Verbindung z.B. `>ping host`.

- **einige** Eigenschaften von ICMP:
  - Fixer Bestandteil von IP.
  - Gibt Auskunft über Fehler bei der Behandlung von IP-Packeten.
  - Macht das IP Protokoll **nicht** zuverlässiger.
  - ICMP Meldungen werden nicht beantwortet (mit Ausnahmen).
  - Für fragmentierte IP-Packete werden ICMP Meldungen nur verschickt, wenn Fehler beim ersten Fragment auftreten.
  - ICMP Fehlermeldungen werden **nie** für Packete verschickt, die an *broadcast* oder *multicast* Adressen gesendet wurden.
  - ICMP Meldungen die **unbekannten Types** sind werden stillschweigend verworfen.

- Man unterscheidet Query und Error Messages.

ICMP Query Messages	ICMP Error Messages
Echo	Destination unreachable
router advertisement	source quench
router solicitation	redirect
time stamp	time exceeded
information	parameter problem
address mask	

- ICMP Meldungen werden als IP Packete gesendet.
  - Die Protokolnummer ist immer **eins** (ICMP).
  - Das `Type-of-Service` Feld im Header ist **null**.
- Das Datenfeld beinhaltet die aktuelle ICMP Meldung.
- Länge der ICMP Fehlermeldung:
  - Jedes Meldung beinhaltet den IP-Header . . .
  - und mindestens die ersten acht Datenoktetts des zu behandelnden Datagramms.

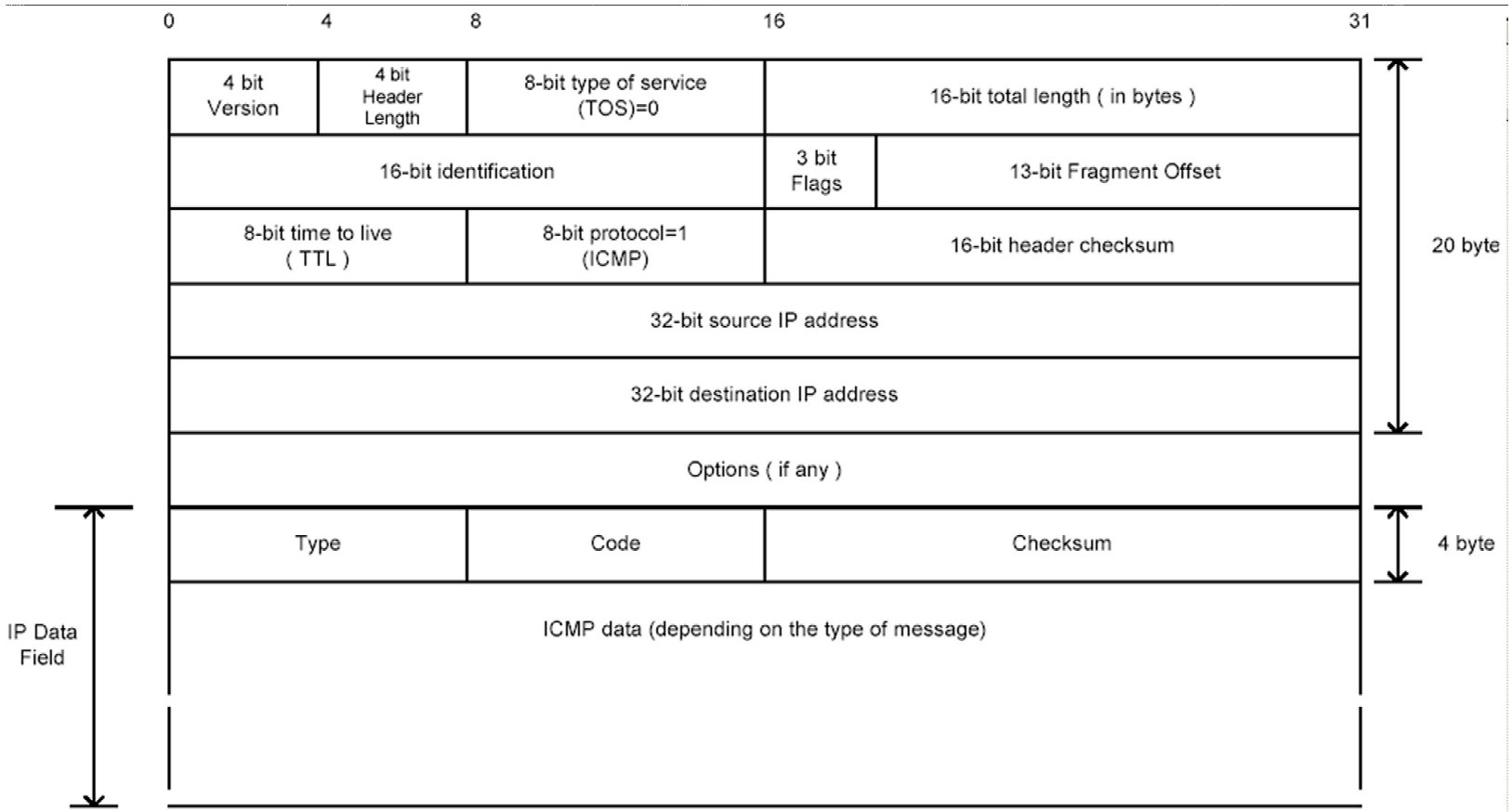

Figure 1: ICMP Message Format

- Das **Type** Feld der ICMP Meldungen legt den Typ fest.
- Der Fehlerkode wird im **CODE** Feld festgelegt.
  - Die Interpretation des Fehlerkodes ist abhängig vom Typ der ICMP Meldung:

Type	Name	Code
0	Echo Reply	0 No Code
⋮		
3	Destination Unreachable	0 Net Unreachable 1 Host Unreachable 2 Protocol Unreachable 3 Port Unreachable 4 Fragmentation Needed and Don't Fragment was Set ⋮

ICMP TYPE Field(2/2)

Type	Name	Code
3 ⋮	Destination Unreachable	6 Destination Network unknown 7 Destination Host unknown
5 ⋮	Redirect	0 Redirect datagramm for the network 0 Redirect datagramm for the host
8 ⋮	Echo Request	0 no code
11 ⋮	Time exceeded	0 Time to live exceeded in transit 1 Fragment reassembly time exceeded
33 34 ⋮	IPv6 where-are-you IPv6 i-am-here	

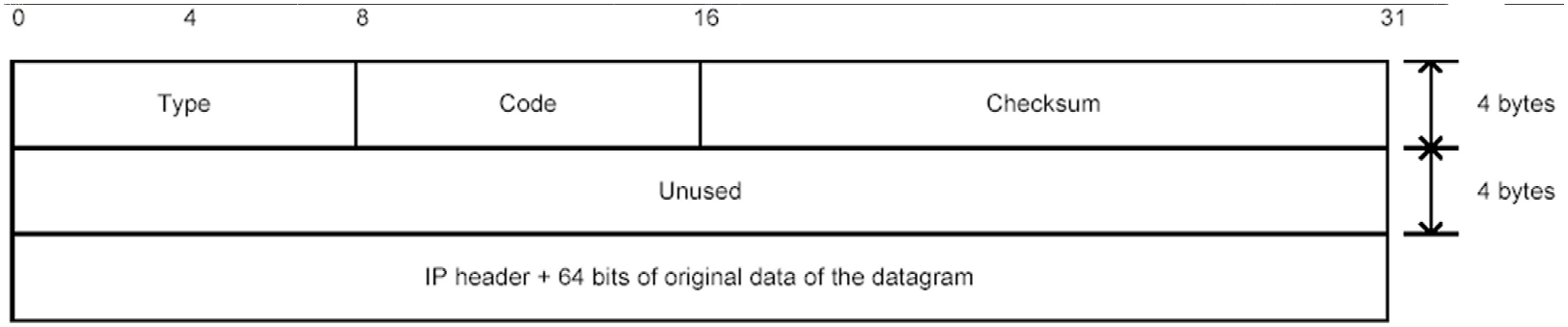

Figure 2: ICMP Error Format

- Checksum - beinhaltet das 1’er Komplement (16 Bit) der Komplement Summe beginnend mit dem ICMP Typenfeld.
  - Für die Berechnung der Checksumme wird diese Feld null gesetzt.
- Das Datenfeld der ICMP Meldung:
  - ICMP Error Meldungen beinhalten einen Teil des originalen IP Packetes für den die Fehlermeldung generiert wurde.
  - Das Datenfeld für ICMP Query Meldungen beinhaltet typenabhängige Informationen.

Host Detection auf Basis von ICMP

Bin da . . . wer noch ??

- Host Detection ist eine Technik, die dem Angreifer Informationen preisgibt, ob und wieviele Rechner in einem Netzwerk erreichbar sind.
  - . . . ist der erste Schritt der Informationsbeschaffung.
  - . . . ist eine Art von Scanning-Technik
  - Die erhaltenen Informationen werden in einem späteren Angriffsszenario genutzt um Zugang zu einem oder mehreren Rechnern zu erhalten.
- Es gibt keine Hilfsprogramme die das Betriebssystem selbst für die Erzeugung von ICMP Query Meldungen zur Verfügung stellt.
  - . . . einzige Ausnahme ist das `ping` Programm, daß zu diesem Zweck mißbraucht werden kann.

ICMP Echo(Type 8)/Reply(Type 0)(1/3)

- ICMP Echo Packete können verschickt werden, um zu sehen, ob eine Ziel IP aktiv ist oder nicht.
  - Hierzu sendet man ein **ICMP Echo (Type 8)** an die Ziel IP und erwartet als Antwort eine **ICMP Echo Reply (Type 0)**.
  - Wird eine solche Antwort zurückgesendet, ist der Zeilrechner aktiv.
  - Keine Antwort bedeutet, daß die IP im Netzwerk nicht erreichbar ist (temporär oder nicht vergeben) . . .
  - . . . oder die Antwort wurde von einem Filter-Programm geschluckt.
- ein `snort` trace eines Ping Vorgangs.

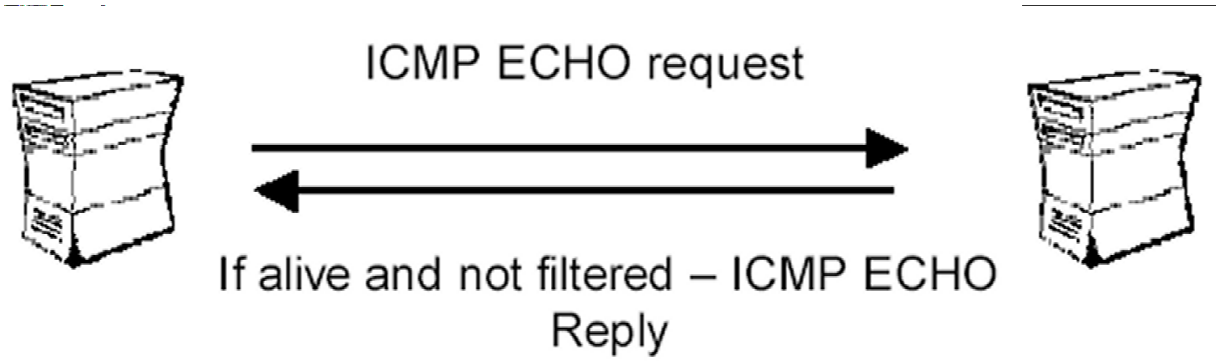

Figure 3: ICMP Echo Mechanism

```
05/14/01-11:55:30.171542 172.18.2.201 -> 172.18.2.200
TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:58628 Seq:768 ECHO
82 9D FF 3A 5C 9E 02 00 08 09 0A 0B 0C 0D 0E 0F ...:\.............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#$%&'()*+,-./
30 31 32 33 34 35 36 37  01234567
```

ICMP Echo(Type 8)/Reply(Type 0)(3/3)

```
05/1
ICMP TTL:255 TOS:0x0 ID:769 IpLen:20 DgmLen:84
4/01-11:55:30.171542 172.18.2.200 -> 172.18.2.201
Type:0 Code:0 ID:58628 Seq:768 ECHO REPLY
82 9D FF 3A 5C 9E 02 00 08 09 0A 0B 0C 0D 0E 0F ...:\.............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#$%&'()*+,-./
30 31 32 33 34 35 36 37  01234567
```

Broadcast ICMP(1/2)

- Eine einfache Technik um eine ganzes Netzwerk zu erforschen ist das aussenden eines ICMP Echo Packetes an die Broadcast Adresse des Ziel Netzwerks.
  - Die Anfrage wird an alle im Netzwerk befindlichen Rechner weitergereicht. Alle Rechner im Netzwerk senden dann ihre Antwort an den Sender zurück.
  - Diese Technik der Host Detection wird nur mehr von einigen Unix bzw. Unix-like Systemen unterstützt.
  - MS Windows basierende Maschinen generieren keine Antwort auf solche Anfragen.
- Das verwerfen von solchen Anfragen ist kein fehlerhaftes Verhalten, denn im **RFC 1122** heist es, das solche Packete stillschweigend verworfen werden **können**.

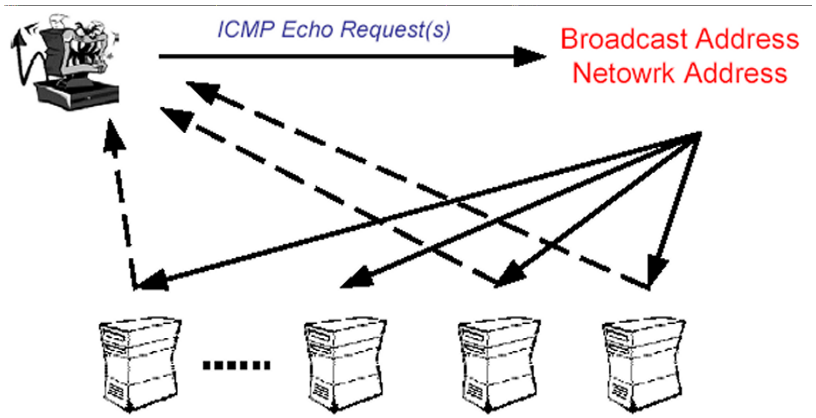

Figure 4: Broadcast ICMP Technik

```
[root@localhost /root]# ping -b 172.18.2.255
WARNING: pinging broadcast address
PING 172.18.2.255 (172.18.2.255) from 172.18.2.201 : 56(84) bytes of
data.
64 bytes from 172.18.2.201: icmp_seq=0 ttl=255 time=6.380 msec
64 bytes from 172.18.2.200: icmp_seq=0 ttl=255 time=6.444 msec (DUP!)
64 bytes from 172.18.2.254: icmp_seq=0 ttl=255 time=6.469 msec (DUP!)
64 bytes from 172.18.2.29: icmp_seq=0 ttl=64 time=6.493 msec (DUP!)
...
```

- Als Inverse Mapping wird eine Technik bezeichnet die verwendet wird, um den Aufbau eine internen Netzwerkes zu bestimmen, welches durch ein Filter geschützt wird.
  - . . . gewöhnlich ist so ein Filter ein Router mit einer Zutritts-Kontroll-Liste.
- Vorgehensweise:
  - Man schickt Packete zu Rechnern deren IP's möglicherweise im Adressraum des Netzwerkes liegt.
  - bekommt der Router ein Packet mit einer IP adresse, die nicht im Netzwerk liegt, antwortet er mit einer **ICMP Host Unreachable** Meldung oder mit **ICMP Time Exceeded error** Meldung.
  - Bekommt man keine Antwort auf die Anfrage, so kann man annehmen, das diese IP im Netzwerk existiert.

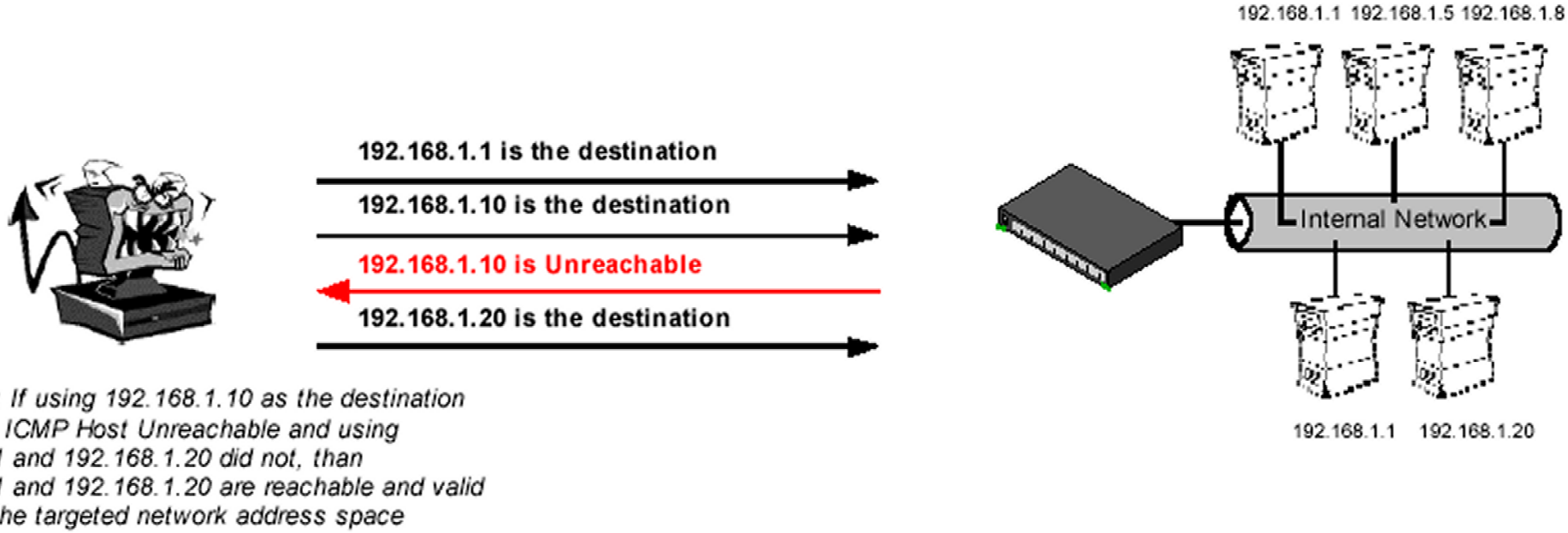

Figure 5: Inverse Mapping Technik

Passive Fingerprinting, eine Einführung

. . . wirklich nur kurz angerissen

- Passive Fingerprinting zielt darauf ab, die interne Struktur eines Netzwerkes zu erforschen (Aufbau, OS, Dienste, offene Ports, etc.)
- . . . Man bedient sich hierbei Informationen die von einem **Sensor** gesammelt werden.
- Der Informationsfluß ist gegenüber aktiven Fingerprinting **indirekt**.
- Der Standort des Sensors unterscheidet zwei Arten von passive Fingerprinting:
  - Der Sensor im internen Netzwerk.
  - Der Sensor in der DMZ.

- Der Standort des Sensors hat entscheidenden Einfluß auf die erhaltene Information.
  - Informationen über E-Mail Server, DNS, File Server, DHCP, jede Kommunikation mit dem Internet und der DMZ, können nur vom Sensor im internen Netz gesammelt werden.
  - Informationen über interne Kommunikation und deren Servises in der DMZ werden können von Sensoren in der DMZ gesammelt werden.

- Systeme erkennen, die nur kurz aktiv sind.
- Der Rechner der Passive FP betreibt kann nicht so schnell gefunden werden.
- Es ist möglich Services jenseits von Filterprogrammen zu entdecken.
- Eine Aktivität des Sensors führt nicht unweigerlich zum Einbruch der Netzwerkperformance.
- . . .

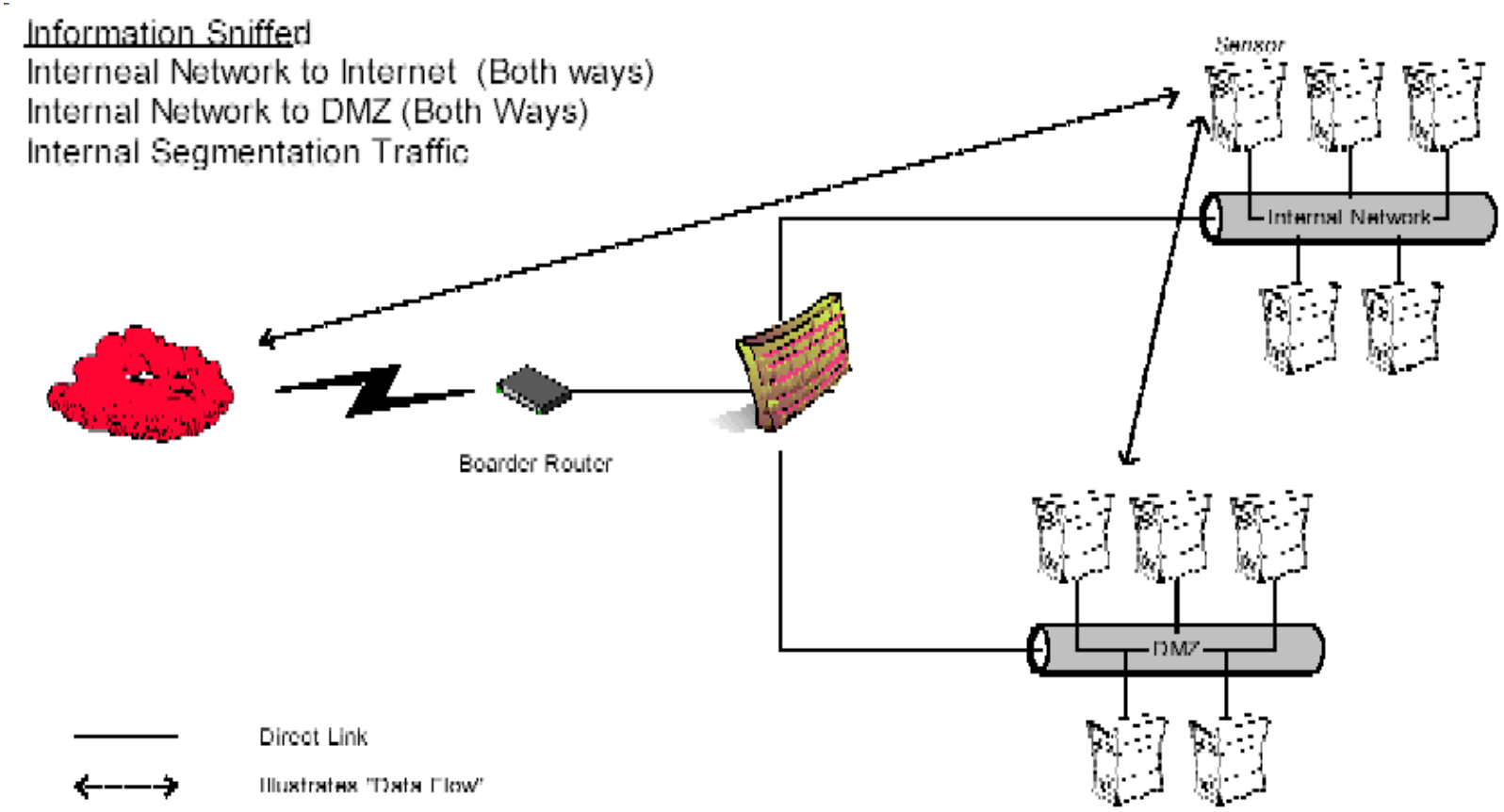

Figure 6: Sensor im internen Netzwerk

. . . finally()

Schlußworte

- Der Autor
  - **Ofir Arkin**
  - ICMP usage in Scanning[1].
  - SecurityIPTelephonyNetworks[2].

[1] http://www.sys-security.com
[2] http://www.sys-security.com

- **Danke für Ihre Aufmerksamkeit**