

# **S t u d i e n a r b e i t**

## **Anschluß gefährdeter Objekte an das Internet**

*Die Alchimie der Neuzeit?*

Andreas Haug <me@this.net>

Prof. Dr. W. Rosentiel  
Lehrstuhl für technische Informatik  
Fakultät für Informatik, Universität Tübingen

# Bearbeitung

- Problemstellung erkunden
  - Bücher, Konferenzen, Web, Berichte
- Gefundene Lösungen evaluieren
  - Geschichte, Einbruchversuche (K/G-RZ, BZ)
- Verbesserungen vorschlagen und prüfen
  - Bauen und kaputt machen... „Brandsatz98“
- Zusammenschreiben
  - „Firewalltechnik für Großbanken“

# Problem

„Sicherheit? Hacker? Kein Problem!  
Wir haben doch damals diese Firewall  
gekauft...“

+ Vertrauen in Hersteller  
+ Vertrauen in Zulieferer  
+ Statisches Weltbild

---

= Desaster

*„Herr Müller! Gehen sie  
ganz schnell in den Keller  
und ziehen sie das Kabel  
zum Internet. Jetzt gleich!!!“*

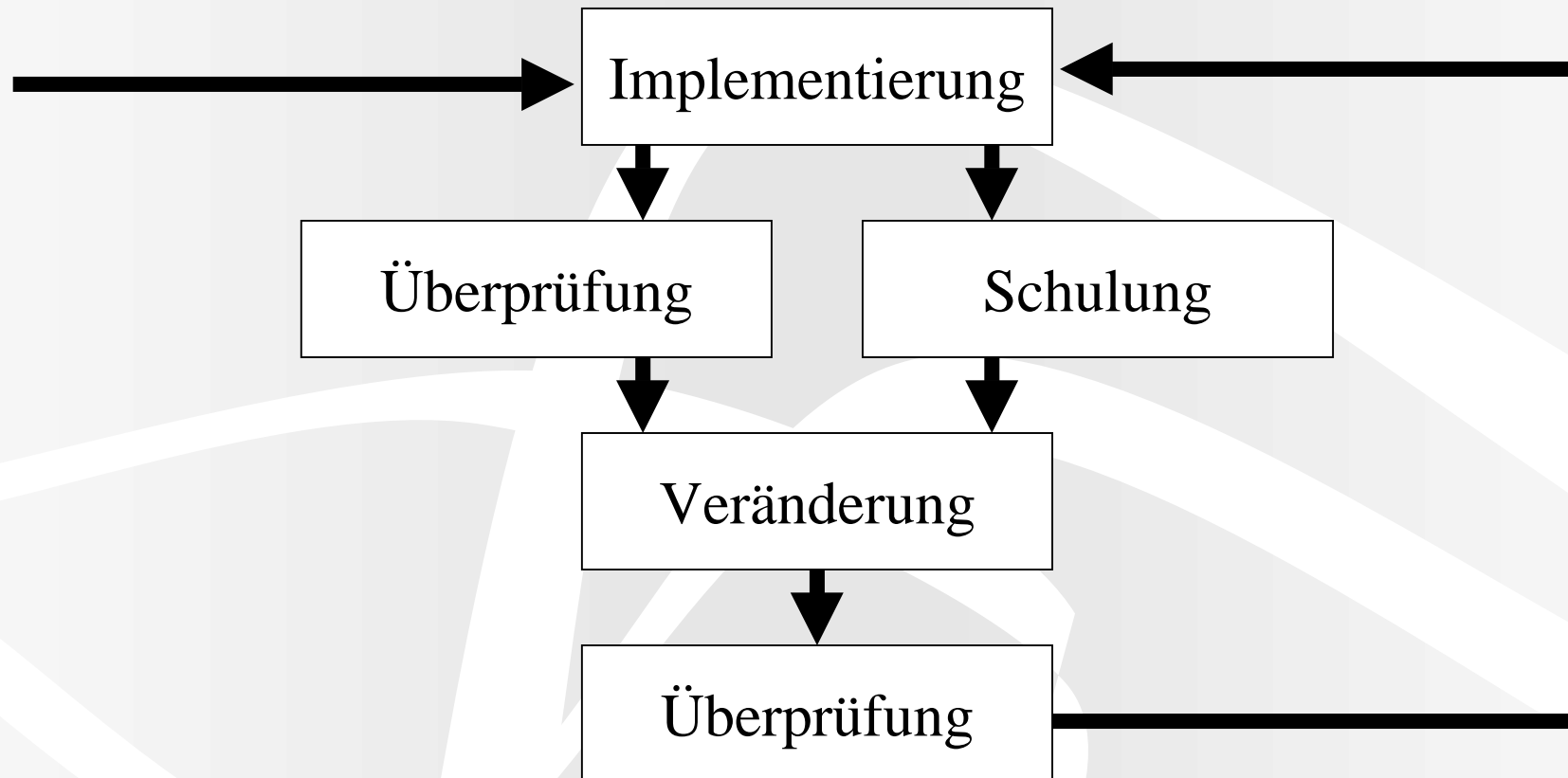
# Angriffe

- Verfügbarkeit (aka Denial Of Service)
  - Land, Boink, Teardrop, SYN-Flood, POD, ...
- Eindringen & Fälschen
  - Buffer Overflows (Exchange, Bind, Imapd,...)
  - Hijacking/Spying (Telnet, SMB, PPTP, ...)
  - Trojaner ‚pflanzen‘ (Java, ActiveX, Viren, ...)
  - Social Engineering („Known Secrets“)
- Impersonation
  - DNS Cache / Proxy Poisoning

# „Richtiges“ Vorgehen

- Warum (komplett) ans Internet?
  - Unbedingt benötigte Dienste ermitteln
  - Alternativen? Sicherheit ist teuer!
- Security Policy
  - Risiken, Maßnahmen, Restrisiken, Verhaltensweisen → Bewußtsein
- Implementierung
  - Tiger-Team Test (auch „Red-Team“ genannt)
- Plug, Pray & Watch

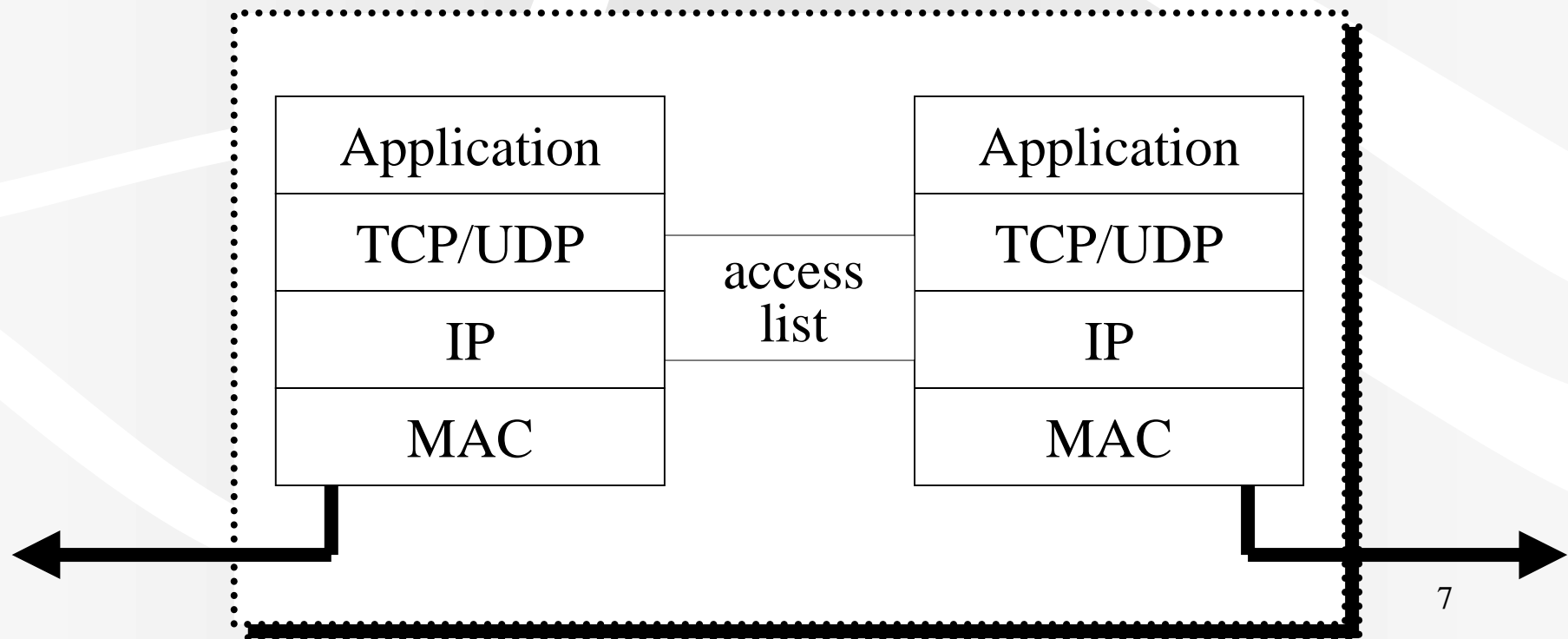
# „Richtiges“ Vorgehen (2)



Security is a process, not a state!

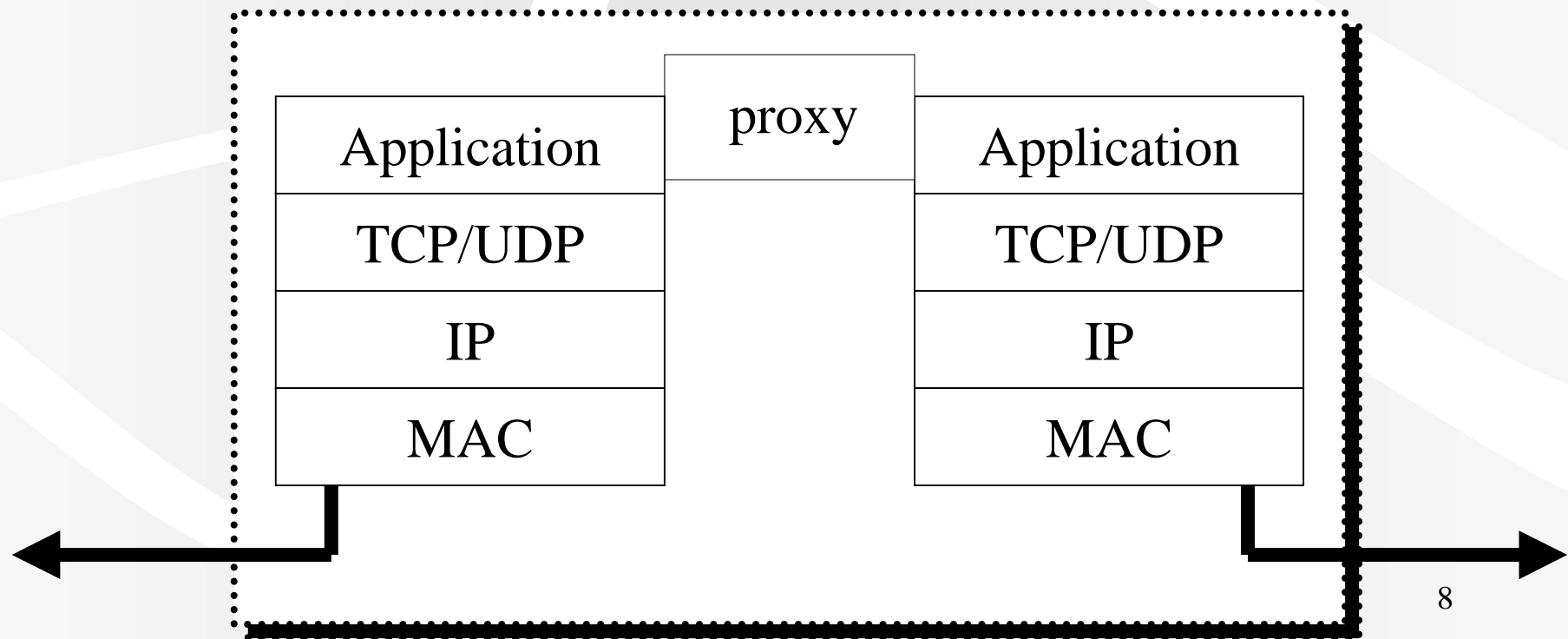
# Firewallkomponenten

- Paketfilter („Screening Router“)



# Firewallkomponenten (2)

- Dual (Multiple) Homed Bastion Host aka Application Level Firewall (ALF)



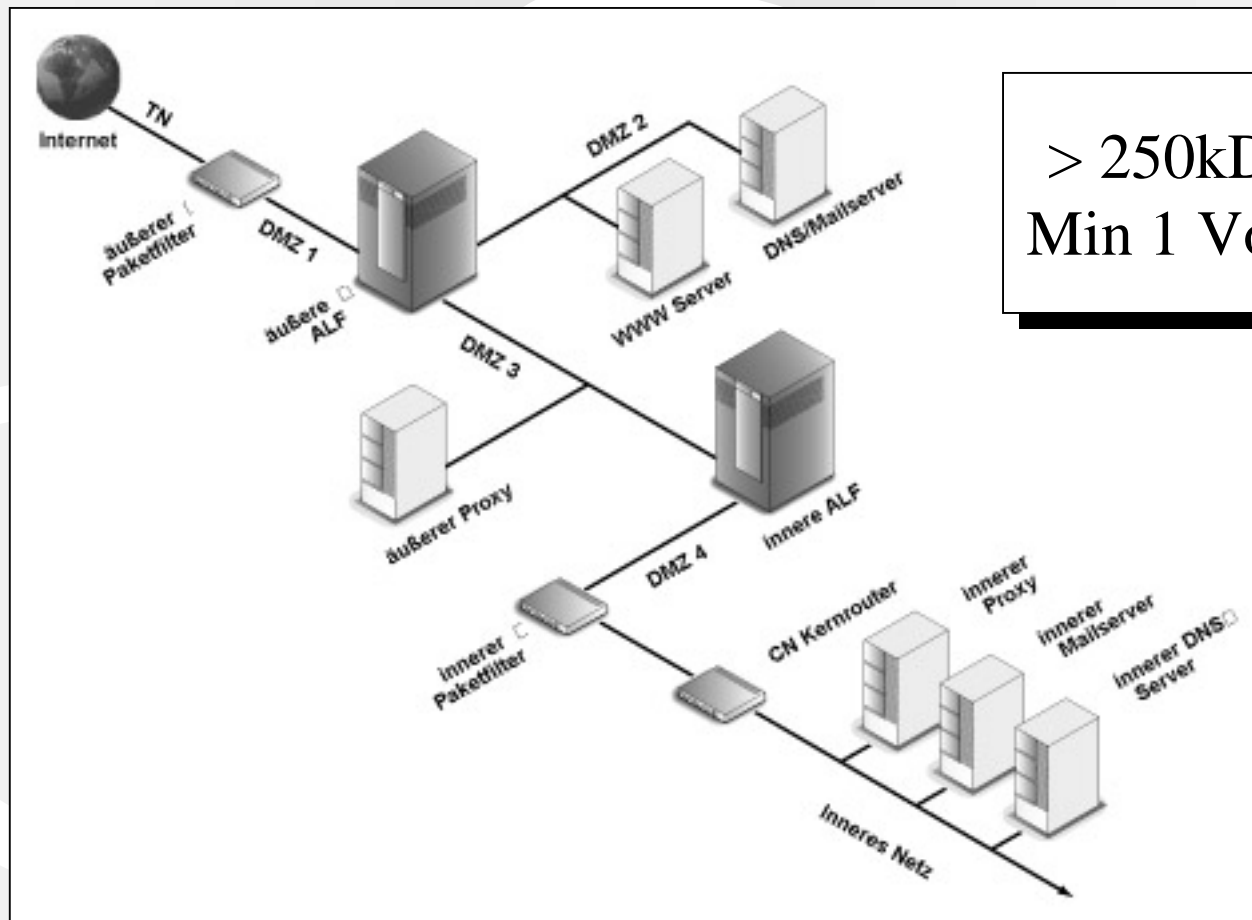
# Firewallkomponenten (3)

	<b>Paketfilter</b>	<b>ALF</b>
<b>Verständnis</b>	Pakete	Transaktionen
<b>Komplexität</b>	Gering	Hoch

# Firewalldesign

- Umsetzung der Security Policy (!)
- Mehrstufiger Aufbau
  - Komponenten schützen sich gegenseitig
  - Kein Vertrauen zwischen Komponenten
  - Wo möglich ‚Quarantänestationen‘
- Baselineing & Intrusion Detection (1998+)

# Firewallvorschlag Projekt „SDL“



> 250kDM Invest  
Min 1 Vollzeitkraft

# (Meta-) Ergebnis

- Nachträgliche Sicherung i.d.R. nicht gut möglich (→ Konzeptionelle Probleme)
- Innere Sicherheit i.d.R. nicht vorhanden und nicht implementierbar (SMB, Routing, ...)
- Weites, teilweise unerschlossenes Feld welches stark wächst
  - Neue Löcher/Angriffe werden gefunden
  - Man setzt noch auf Gefühl/Gespür