Network Security

www.pc24berlin.de/sicherheit.htm

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Warum ist dieses Thema von Interesse?

IT ist Bestandteil des täglichen Lebens für Behörden,

Geldtransfer, Geschäftsprozesse...

Abhängigkeit von diesen Computersystemen bzw. Netzwerken.

Ein Ausfall bewirkt weitreichenden Schaden

Warum ist dieses Thema von Interesse?

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Aus dieser Abhängigkeit heraus stellen sich folgende Fragen:

I. Welche Möglichkeiten gibt es, sein Netzwerk zu schützen?

II. Was sollte man beachten?

Passive und aktive Attacken

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Aus Data and Computer Communications von William Stallings machen wir folgende Einteilung:

Passive Attacken:

I. Abhören:
- -einer einzelnen Verbindung,
- -eines ganzen Rechnernetzes.
  (tools:Kisment,Ethereal/wireshark)

II. Analyse des Netzwerksverkehrs
  (Krypto-Analyse)

Passive/Aktive Attacken

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Aktive Attacken

-Manipulation des Datenstroms
-Erzeugen ungültiger Verbindungen
-Aufteilung in 4 Typen

I.Masquerade: Verbergen der Identität:Manipulation des IP Headers

II.Replay: Erneutes Versenden aufgezeichneter Daten.(WEP crack)

III.Modifcation of messages: Abändern von Nachrichten.

IV.Denial of Service: Störung des Arbeitsprozesses durch Schwachstellen.(dienst, OS)

Einsatz von Kryptographie

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

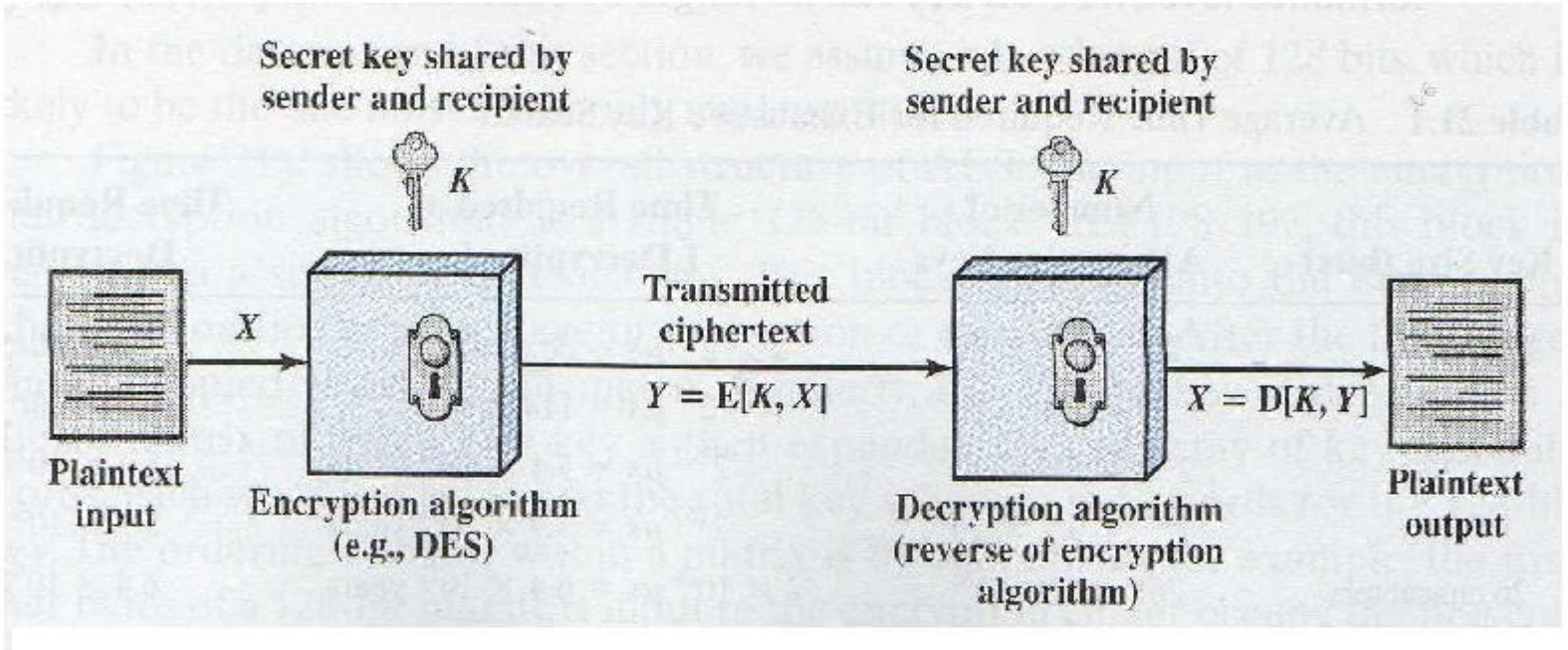
Kryptographie als Mittel gegen passive Attacken.

I. Symmetrische Verfahren.

II. Asymmetrische Verfahren
In dieser Präsentation nicht näher betrachtet

Einsatz von Kryptographie

Symmetrische Verfahren



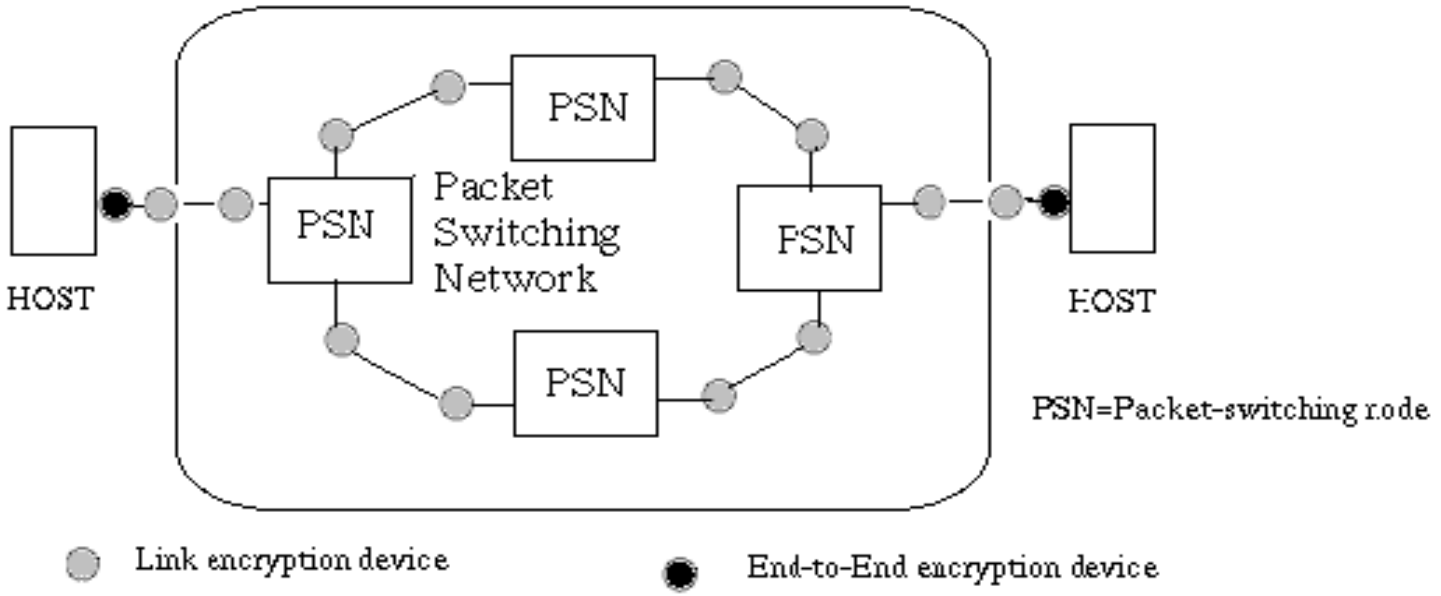
Stallings:Data and Computer Communication Seite 705

Sender und Empfänger teilen gemeinsame Schlüssel
Anforderung

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Einsatz von Kryptographie

Anwendung



Stallings:Data and Computer Communication Seite 710 nachempfunden

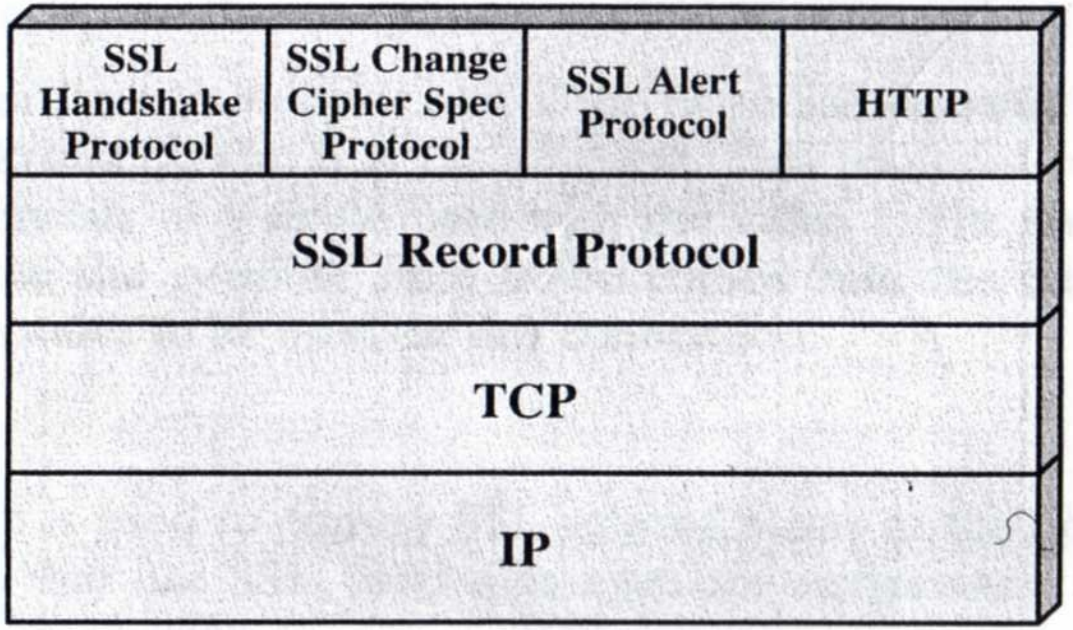
Erschwert passive Attacken und erhöht damit die Sicherheit im Netz.
Traffic Padding unterstützt diese nochmal.

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Einsatz von Kryptographie

Anwendung

end-to-end encryption mit TLS/SSL



Stallings:Data and Computer Communication Seite 728

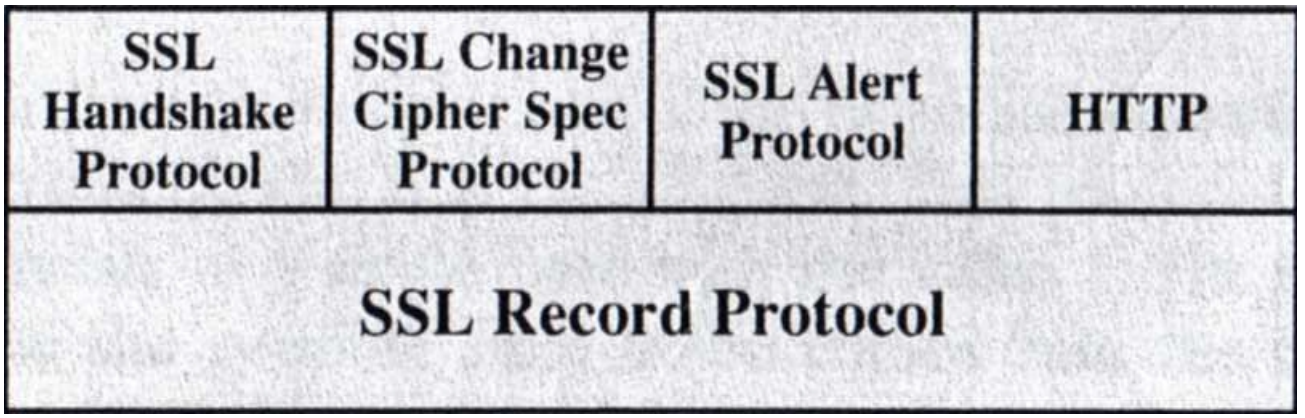
SSL ist im OSI/ISO Schichtenmodell über Transportschicht.

Bietet höheren unsicheren Diensten wie ftp,imap,www,pop,... Verschlüsselung und Authentisieren an.

Einsatz von Kryptographie

Anwendung

TLS ist unterteilt in verschiedene Protokolle



Stallings:Data and Computer Communication Seite 728

1. SSL Record Protokoll:Symmetrisches Verschlüsseln
2. SSL Handshake Protokoll: handelt den verwendeten Schlüssel aus.
3. Alert Protokoll: Austausch von SSL spezifischen Nachrichten
4. Cipher Spec :Dient zum Aufrechterhalten der verwendeten Verbindung

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Firewalls tragen immens zur Sicherheit von Netzen bei.

Die Vorschläge und Einteilung ortientieren sich an:

http://cone.informatik.uni-freiburg.de/teaching/vorlesung/systeme-II-s07/folien/systeme-II-11.ppt

Netzwerk Firewalls:
- Trennung der Netze.

Host Firewalls:
- Überwachung des Systems(Traffic,Prozesse).
- Schutz von außen wie von innen.

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Firewalls

IP (IPv4)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|        Total Length           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Identification         |Flags|     Fragment Offset     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |       Header Checksum         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Options                   |     Padding   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Umsetzungen : **Paketfilter**:

-Benutzen Information,
die im Header stehen.

In TCP/IP wären das dann = >

TCP

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Bekannte Paketfilter:
-pf von openBSD

-ipfw von freeBSD

-iptables für Linux

·http://cone.informatik.uni-freiburg.de/teaching/vorlesung/systeme-II-s07/folien/systeme-II-09.ppt

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Bastion Host

-Spezielle Hochsicherheitssysteme.

-Dienstangebot für externes Netz.

-offenes Ziel

http://www.aeria.phil.uni-erlangen.de/photo_html/asterix.jpg

Firewalls

Proxy

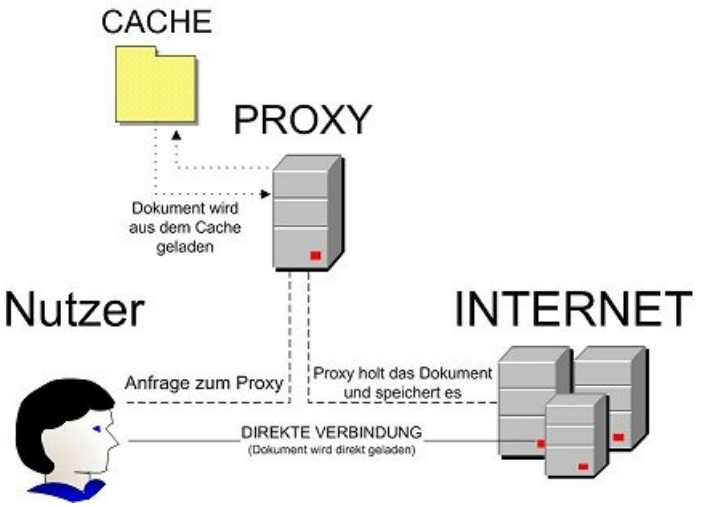
-Umleitung des Datenstroms auf speziellen Rechner

-Antworten auf alle Anfragen gehen auf Proxy.

-Proxy kann cachen

-Sicherung durch Content-filter.

-Sicherung durch IDS Systeme



http://www.freetagger.com/wp-content/uploads/2007/10/proxyserver.png

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

NAT: Network Address Translation

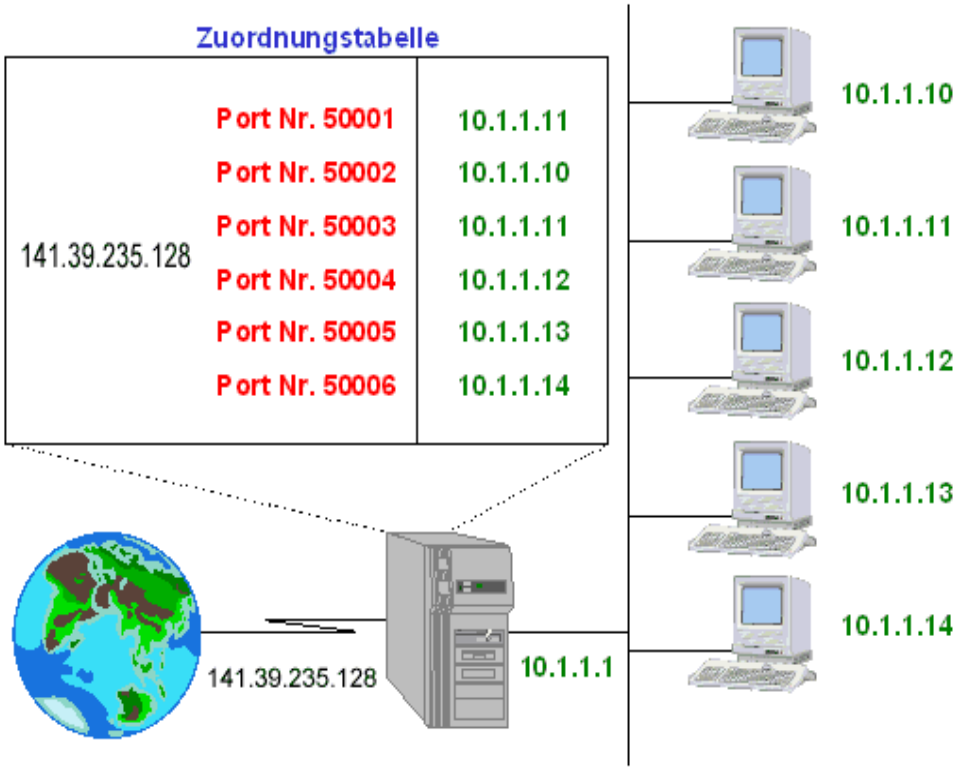
-bei NAT oft gemeint NAT/PAT

-Zuweisung einer Adresse für ein ganzes Netz-Segment

-Oft anzutreffen in IP Netzen

-Externe Rechner können keine Information über die innere Struktur des Netzes erhalten.

-Alle Rechner im internen Rechnernetz wirken wie ein Rechner



http://www.netzmafia.de/skripten/netze/netz8.html

Niemand ist sicher

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica

Bis jetzt nur Absicherung betrachtet!

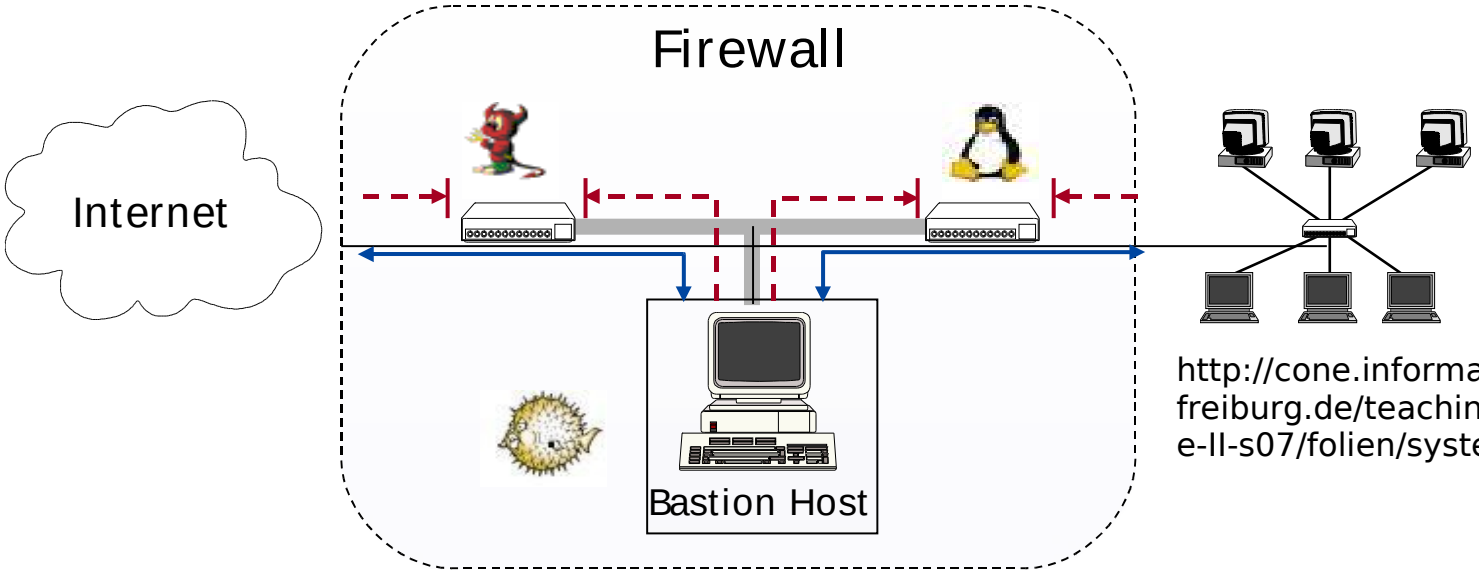
Gegenmaßnahmen bei erfolgreichem Angriff.

Schadensbegrenzung?

Isolation?

Screened Subnet

Albert Ludwigs Universität Freiburg
Institut für Informatik
Ivo Malenica



http://cone.informatik.uni-freiburg.de/teaching/vorlesung/systeme-II-s07/folien/systeme-II-11.ppt

Externes Netz | DMZ | interes Netz
Nutzung verschiedener Elemente erhöhen die Sicherheit

Ende

Danke für die Aufmerksamkeit

Gibt es noch Fragen?