

# A Taxonomy of Web Attacks

## **Eine Taxonomie für Web Attacken**

Ein Vorschlag von Gonzalo Álvarez und  
Slobodan Petrovic [1]

# A Taxonomy of Web Attacks

## Gliederung

1. Begrifflichkeiten (Taxonomie, Web Attacke) und Ziel
2. Web Attacken im Detail / Motivation
3. Die Taxonomie im Detail
4. Mögliche Anwendungen der Taxonomie
5. Kritik

# 1. Begrifflichkeiten

## **Def.: Taxonomie (1/2)** [2]

- „eine Einteilung von Dingen“
- Begriff insb. in der Biologie verwendet (Organismen)
- Anwendung auch in der Linguistik und generell des Wissensmanagements

# 1. Begrifflichkeiten

## Def.: Taxonomie (2/2) [1] [3]

### Hier:

- Eine **Taxonomie** ist eine Strukturierung von Begriffen und deren Beziehungen in einem (meist hierarchischen) Ordnungssystem.
- Klassifizierung ist der Prozess der Anwendung einer Taxonomie

# 1. Begrifflichkeiten

## Eigenschaften einer guten Taxonomie [1]

### Die Klassifizierungskategorien...

- sind sich gegenseitig ausschließend
- decken alles ab
- sind wiederholt anwendbar
- sind nützlich
- sind akzeptiert

# 1. Begrifflichkeiten

**Def.: Web Attacke [1]**


## **Formal:**

- Ist ein Angriff [auf Server bzw. deren Software] unter ausschließlicher Nutzung des HTTP / HTTPS-Protokolls

**→ Hierbei besteht eine Vielzahl verschiedener Möglichkeiten**

# A Taxonomy of Web Attacks

## Gliederung

1. Begrifflichkeiten (Taxonomie, Web Attacke) und Ziel
-  2. **Web Attacken im Detail / Motivation**
3. Die Taxonomie im Detail
4. Mögliche Anwendungsmöglichkeiten der Taxonomie
5. Kritik

## 2. Web Attacken im Detail / Motivation

### Tools für Webattacken [4]

#### **Basis:**

- **Browser**
- Texteditor
- Kommandozeilen - Telnet-Client

#### **Eventuell:**

- „komfortable“ Tools bzw. Telnet-Clients, die Serverantworten übersichtlich darstellen und beim editieren von Anfragen helfen

## 2. Web Attacken im Detail / Motivation

### Basics: Das HTTP-Protokoll (1/3) [5]

#### Ablauf eines Webseitenaufrufs:

- Client / Server Prinzip
- Browser schickt HTTP-Request
- Server antwortet mit HTTP-Response



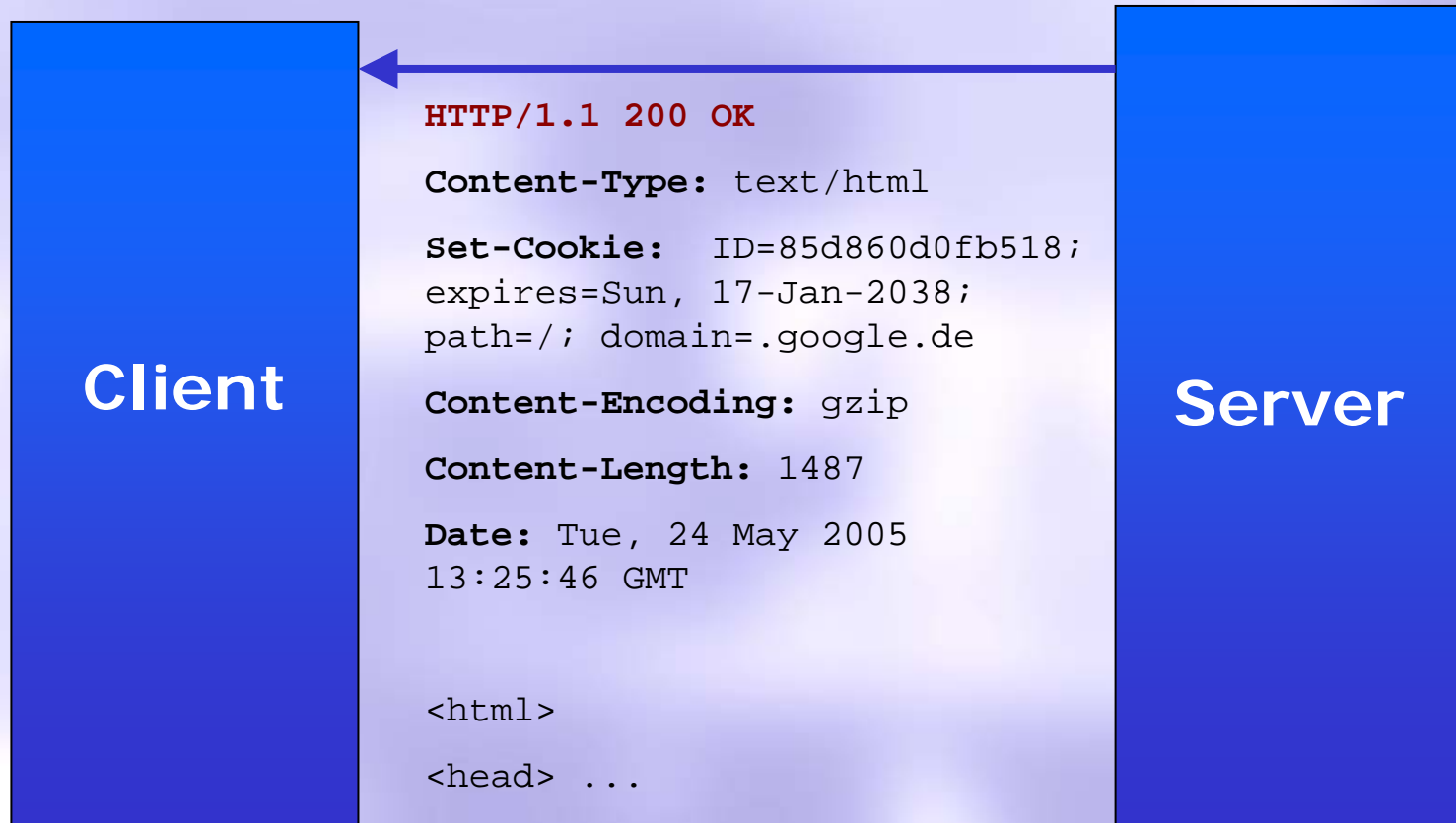
## 2. Web Attacken im Detail / Motivation

### Basics: Das HTTP-Protokoll (2/3) [5]



## 2. Web Attacken im Detail / Motivation

### Basics: Das HTTP-Protokoll (3/3) [5]



## 2. Web Attacken im Detail / Motivation

### Beispiel 1: Eine simple Web-Attacke [4]

#### Szenario:

- Eine Firma möchte den vollen Service ihres Webangebots nur Usern zur Verfügung stellen, die den Firmeneigenen Browser nutzen

#### Verfahren:

- Server-Applikation prüft den gesendeten User-Agent-Header und gibt dementsprechend (ausführliche / Abgespeckte) Seiten zurück

**Ansatz:** Requestheader fälschen

## 2. Web Attacken im Detail / Motivation

### Beispiel 2: Eine simple, reale Web-Attacke

#### Szenario:

- Ein Student unserer Uni wollte auf seiner Homepage eine Umfrage durchführen, an der jede IP-Adresse nur einmal teilnehmen kann

#### Attacke durch:

- Unix-Shell-Script, das den Header eines Browsers simuliert und Umfragescript von jedem Rechner der Sun-Pools aus aufruft

## 2. Web Attacken im Detail / Motivation

### Beispiel 3: SQL-Injektion (1/2) [6]

#### Szenario:

```
http://www.article.net/cgi-  
bin/findarticle.cgi?ID=42
```

#### Generierte SQL-Anfrage:

```
SELECT author, subjekt, text FROM artikel  
WHERE ID=42
```

## 2. Web Attacken im Detail / Motivation

### Beispiel 3: SQL-Injektion (2/2) [6]

#### Szenario:

```
http://www.article.net/cgi-  
bin/findarticle.cgi?ID=42;UPDATE%20user%2  
0SET%20TYPE="admin"%20WHERE%20ID=23
```

#### Generierte SQL-Anfrage:

```
SELECT author, subjekt, text FROM artikel  
WHERE ID=42
```

```
UPDATE user SET TYPE="admin" WHERE  
ID=23
```

## 2. Web Attacken im Detail / Motivation

### **Taxonomie: Motivation** [1]

#### **Web-Attacken:**


- unterschiedlichste Ansätze und Verfahren
- verschiedenste Ziele der Angreifer
- Fließende Grenze zu ordnungsgemäßer Nutzung der entsprechenden Web-Anwendung

#### **Konsequenz:**

- Klassifizierung der Attacken zu einer Filterung aus der Vielzahl von ordnungsgemäßen Zugriffen nötig

# A Taxonomy of Web Attacks

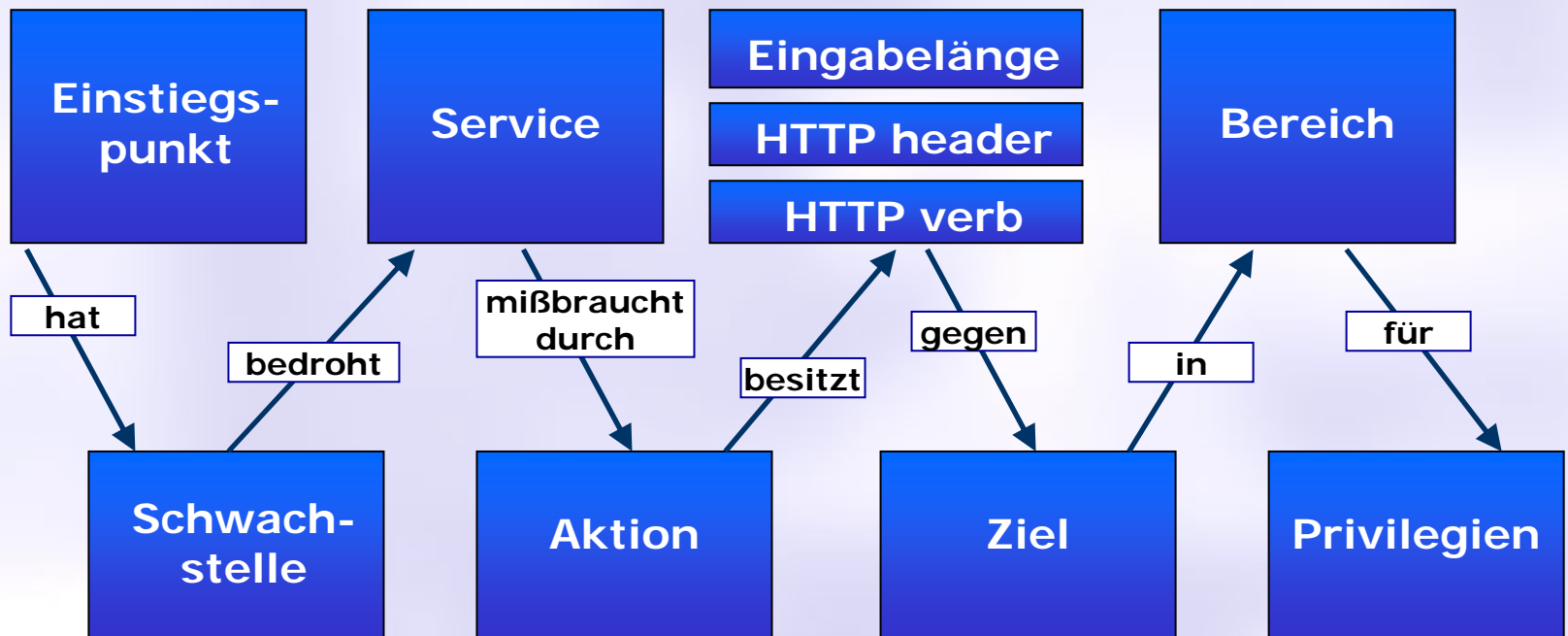
## Gliederung

1. Begrifflichkeiten (Taxonomie, Web Attacke) und Ziel
2. Web Attacken im Detail / Motivation
-  **3. Die Taxonomie im Detail**
4. Mögliche Anwendungen der Taxonomie
5. Kritik

### 3. Die Taxonomie im Detail

## Basis: Der „Attack Life Cycle“ [1]

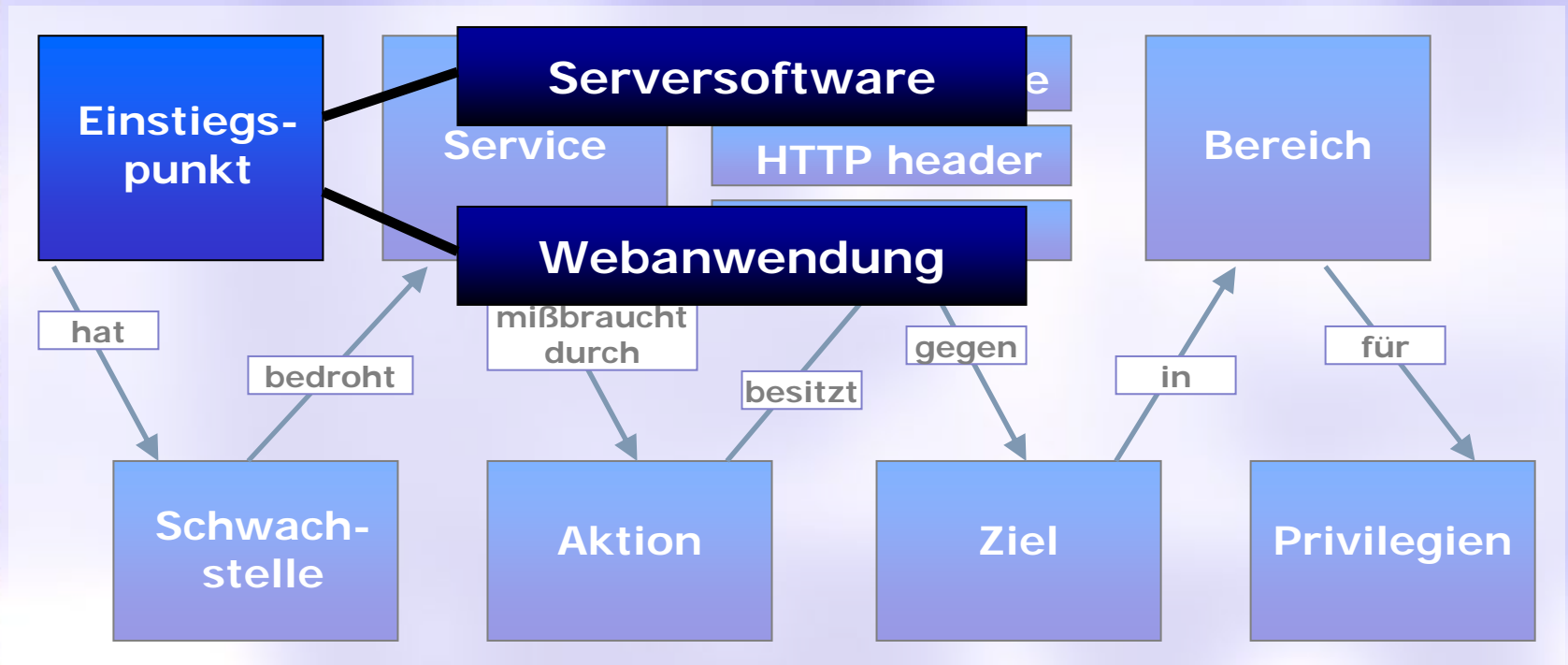
Álvarez und Petrovic's nutzen für ihre Taxonomie ein eigenes Modell für Webattacks - den „**Attack Life Cycle**“



### 3. Die Taxonomie im Detail

## Die eigentliche Taxonomie [1]

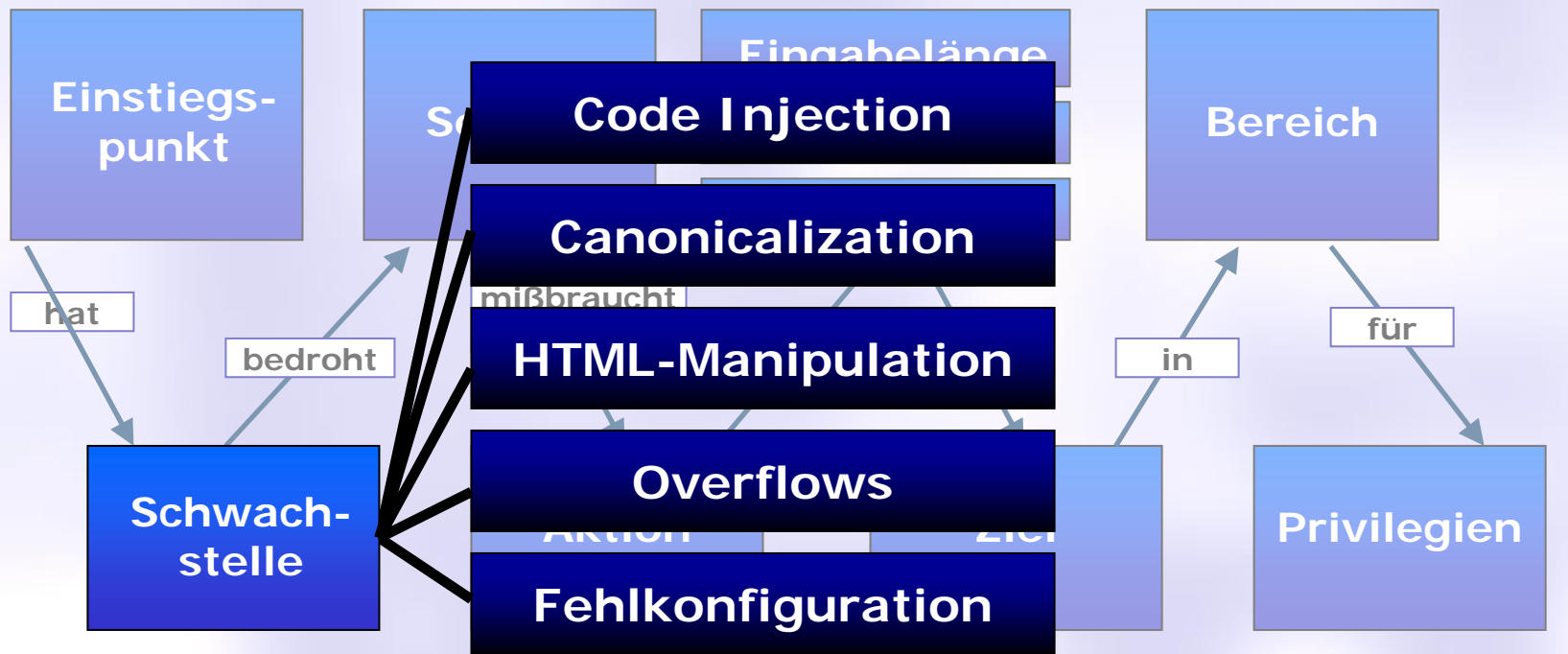
- Grobeinteilung der Attacks: Wo setzt der Angreifer an?



### 3. Die Taxonomie im Detail

## Die eigentliche Taxonomie [1]

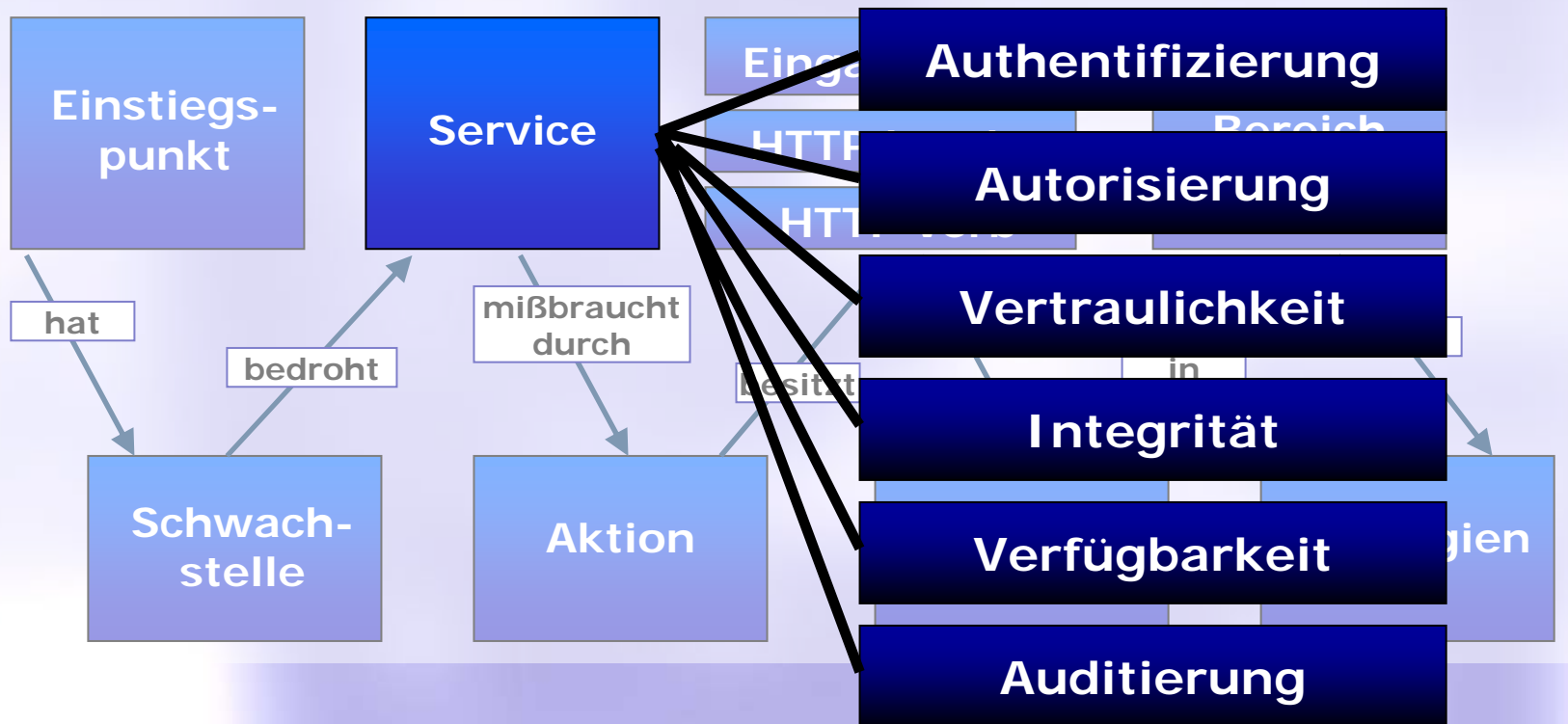
- Feinere Unterteilung: Die ausgenutzte Schwachstelle



### 3. Die Taxonomie im Detail

## Die eigentliche Taxonomie [1]

- Was wird durch die Attacke ausgehebelt?



### 3. Die Taxonomie im Detail

## Die eigentliche Taxonomie [1]

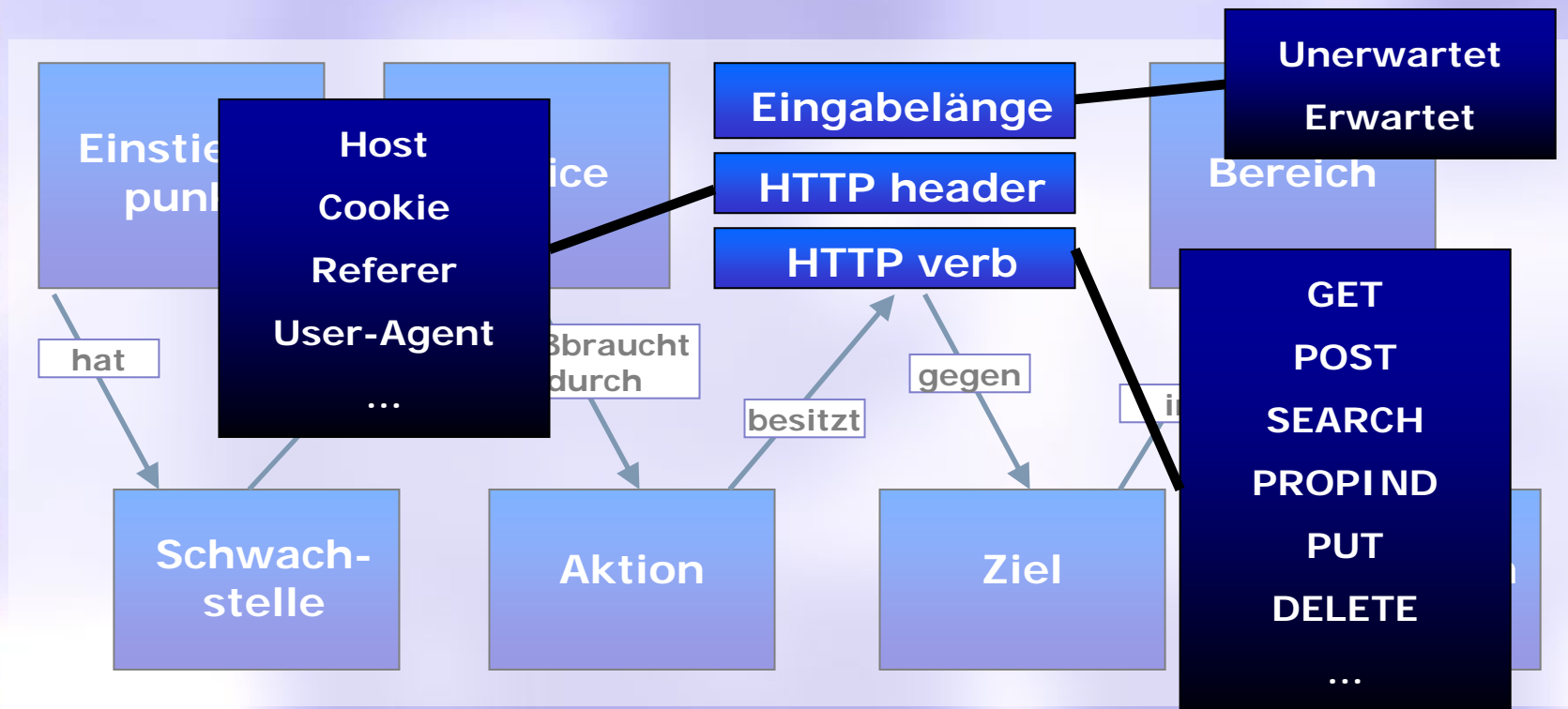
Was wird mit den Daten / Authentifizierung / Webserver gemacht?



### 3. Die Taxonomie im Detail

## Die eigentliche Taxonomie [1]

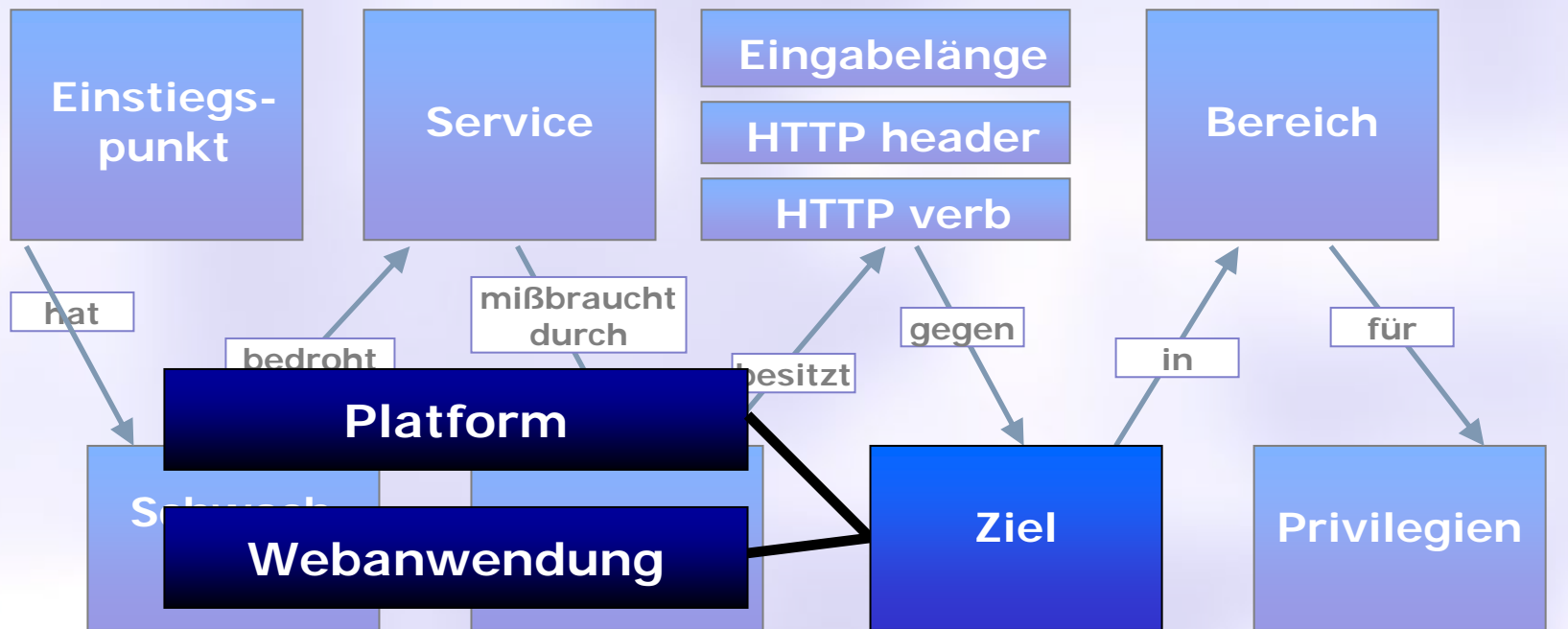
- Welche Eigenschaften besitzt die Anfrage des Angreifers?



### 3. Die Taxonomie im Detail

## Die eigentliche Taxonomie [1]

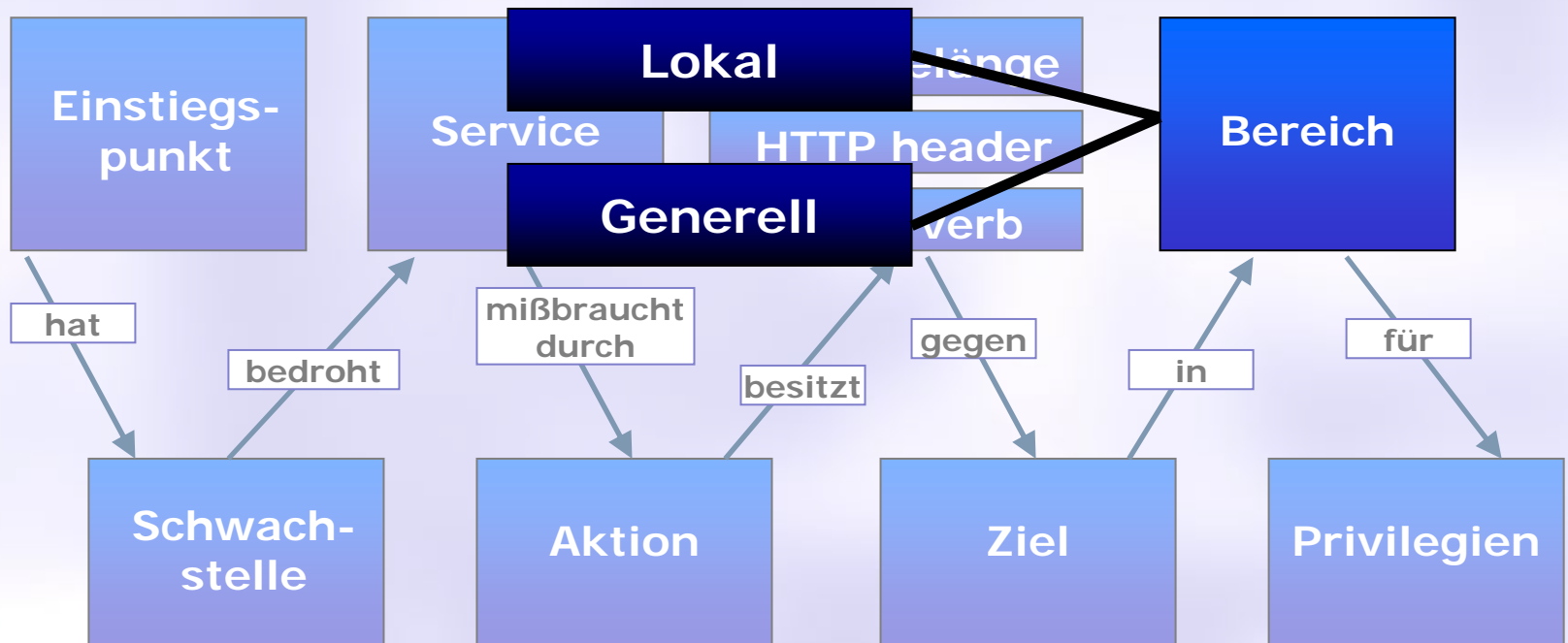
- Was ist von der Attacke betroffen?



### 3. Die Taxonomie im Detail

## Die eigentliche Taxonomie [1]

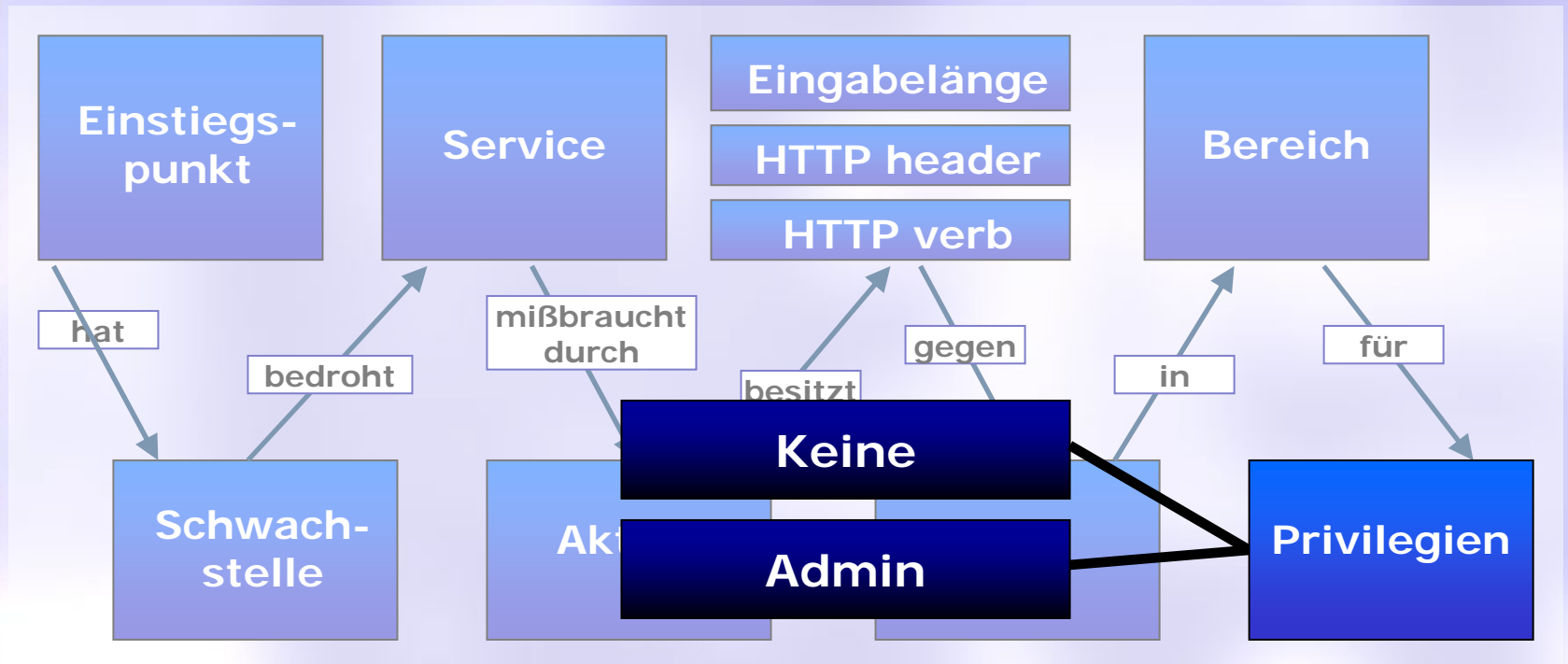
- Wieviele User auf dem Server sind betroffen?



### 3. Die Taxonomie im Detail


## Die eigentliche Taxonomie [1]

- Welche Rechte erwirbt der Angreifer?



# A Taxonomy of Web Attacks

## Gliederung

1. Begrifflichkeiten (Taxonomie, Web Attacke) und Ziel
2. Web Attacken im Detail / Motivation
3. Die Taxonomie im Detail
- 4. **Mögliche Anwendungen der Taxonomie**
5. Kritik

## 4. Mögliche Anwendungen

### **Intrusion Detection Systems [1]**

- Echtzeitanalyse von Angriffen auf Webserver
- Sehr viele (Fehl-)Alarme bei stark attackierten Servern -> Belastung für Admin

#### **Verbesserung:**

- Kodierung der einzelnen Attacken anhand der Taxonomie in 10-stellige Vektoren
- Anwendung von Bildverarbeitungs-algorithmen zur Bestimmung von Häufungspunkten und zeitlichen Trends

## 4. Mögliche Anwendungen

### **Application (Web-) Level Firewalls [1]**


- In die Webanwendung integrierte Firewall, blockt direkt in ihr schädliche Anfragen

#### **These:**

- Für eine schnelle Antwort des Servers auf schädliche Anfragen ist eine Klassifizierung derselben nötig
- Anhand dieser Klassifizierung kann die Schwere einer Attacke effizient bestimmt werden

# A Taxonomy of Web Attacks

## Gliederung

1. Begrifflichkeiten (Taxonomie, Web Attacke) und Ziel
2. Web Attacken im Detail / Motivation
3. Die Taxonomie im Detail
4. Mögliche Anwendungen der Taxonomie
-  5. **Kritik**

## 5. Zusammenfassung

### Kritik

- Es werden von Álvarez und Petrovic mögliche Anwendungen genannt, aber kein konkreter Weg, die Taxonomie in denselben zu nutzen (lediglich Hypothesen ohne Funktionsnachweis)
- Eine Begründung für die Klassifizierung (Statistische Erhebungen? Erfahrung? Willkürlich?) fehlt völlig.
- Es wird nur jeweils ein Request betrachtet (DoS-Attacken nicht erfasst)

## 5. Zusammenfassung

### **Kritik** [7][8]

- Attacken, die andere auf TCP/IP basierende Protokolle nutzen als HTTP(S), werden nicht berücksichtigt

### **Beispiel:**

- „Ping of Death“ (TCP/IP -> ICMP)
  - Webserver, die HTTP nutzen, kommunizieren auch über diese Protokolle
- **Derartige Fehler nicht Kategorisierbar**

# A Taxonomy of Web Attacks

## Referenzen (1/2)

- [1] A Taxonomy of Web Attacks  
*Gonzalo Álvarez und Slobodan Petrovic*  
Spanien / Madrid - Juli 2003  
<http://www.iec.csic.es/>
- [2] Wikipedia - Suchbegriff „Taxonomie“  
<http://de.wikipedia.org/wiki/Taxonomie>
- [3] Virtuelles Software Engineering  
Kompetenzzentrum – „Taxonomie“  
<http://www.software-kompetenz.de>
- [4] Hack this Site  
<http://www.hackthissite.org>
- [5] Das HTTP-Protokoll  
<http://www.elektronik-kompendium.de/sites/net/0902231.htm>

# A Taxonomy of Web Attacks

## Referenzen (2/2)

- [6] Wikipedia - Suchbegriff „SQL-Injektion“  
<http://de.wikipedia.org/wiki/SQL-Injektion>
- [7] ICMP kann TCP/IP Probleme machen  
<http://www.golem.de/0504/37482.html>
- [8] Ping of Death  
[http://de.wikipedia.org/wiki/Ping\\_of\\_Death](http://de.wikipedia.org/wiki/Ping_of_Death)