

# Towards Denial-of-Service Resistant Internet Services

Christian Scheideler

Institut für Informatik

Technische Universität München

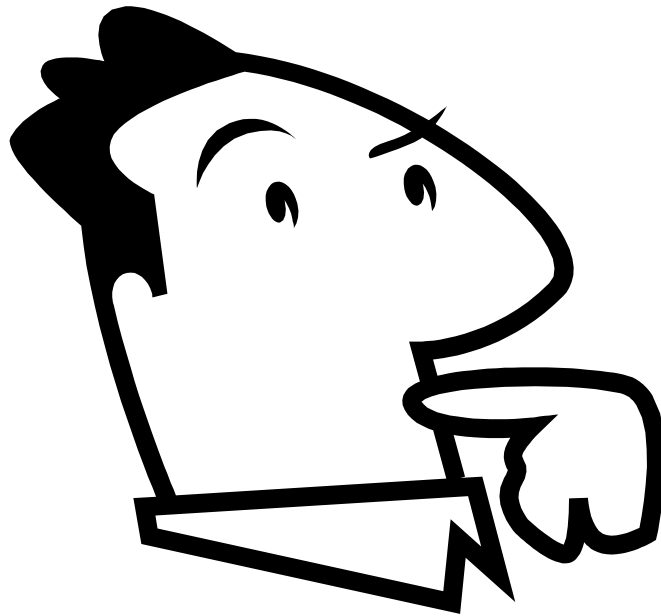
# DoS Attacks

**Wikipedia:** A DoS attack is „an attempt to make a computer resource unavailable to its **intended users**”.



# DoS Attacks

What is an intended user?



# DoS Attacks

What is an intended user?

Algorithmic approach:

- Any user with **admissible behavior**.  
Many stability results on **adversarial**  
behavior within **admissible bounds**.

**bounded attacks**

# DoS-resistant information systems

Past-Insider-Attack: Adversary knows **everything** about system till (unknown) time  $t_0$

Goal: design **scalable** information system so that **ev** **you** inserted or updated **after** **for** (w.h.p.) against any **past-insider** that can shut down a **const** of servers



**bounds!**

# DoS Attacks

What is an intended user?

Algorithmic approach:

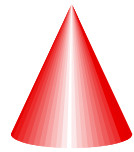
- Any user with **admissible behavior**.  
Many stability results on **adversarial**  
behavior within **admissible bounds**.

**Unbounded** adversarial behavior: **Problem!!**

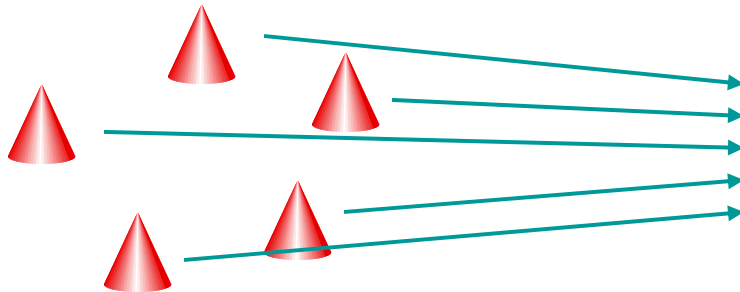
# DoS Attacks

Types of unbounded adversarial behavior:

- Users **violate** admissible behavior



- **Too many** users (Sybil attack)



# DoS Attacks

Unbounded adversarial behavior

Principle of least authority

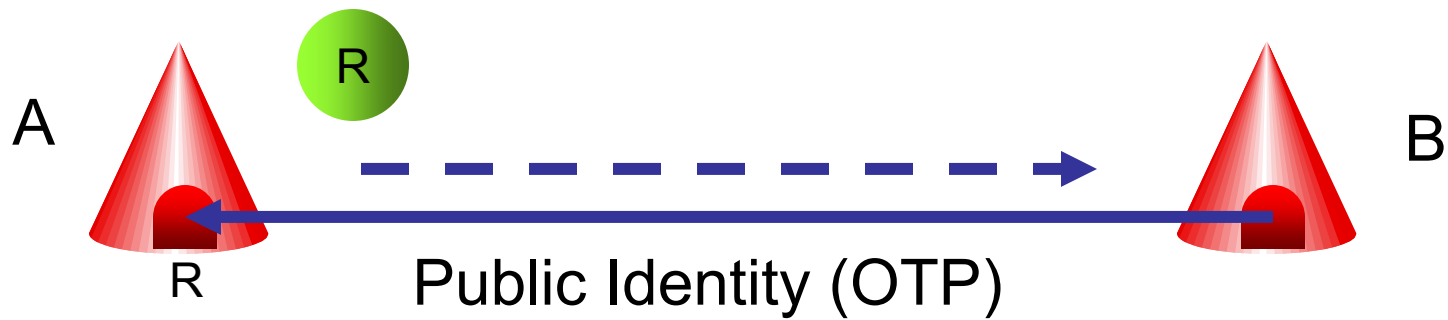
It's all about resource control!



Owner consent and control

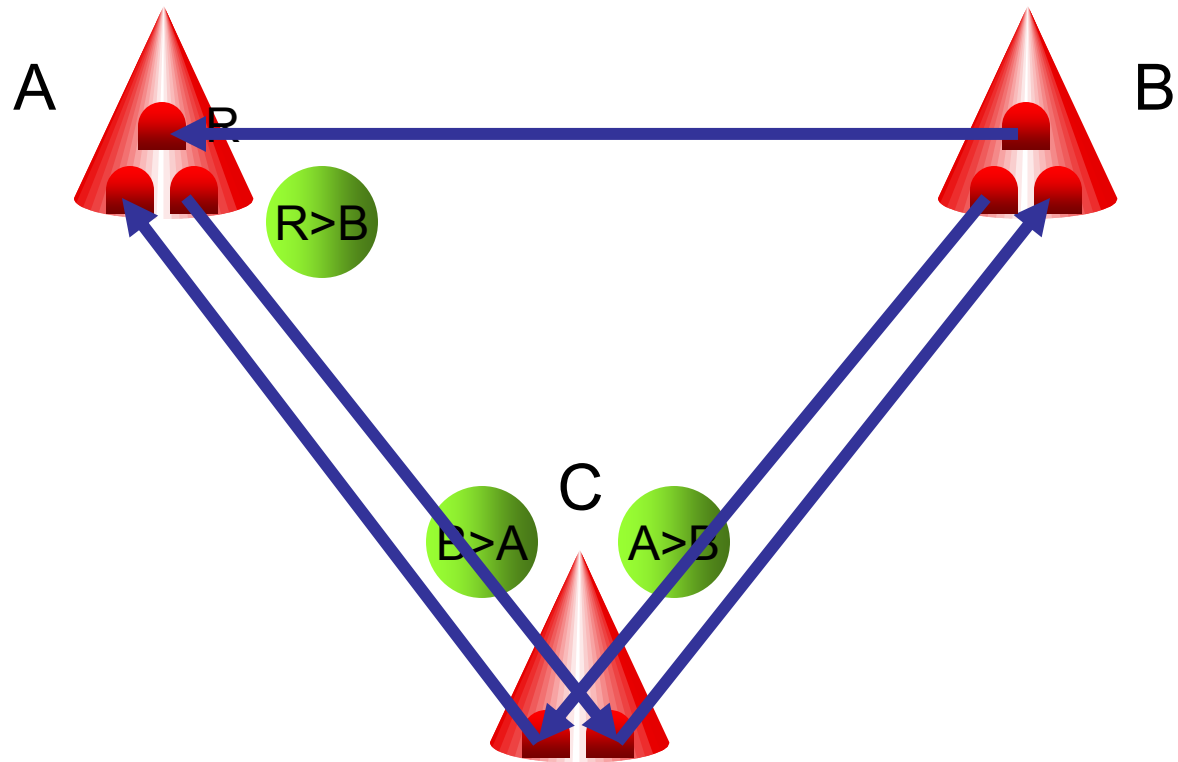
Internet-based **robust** pseudonymity service!

# First Contact

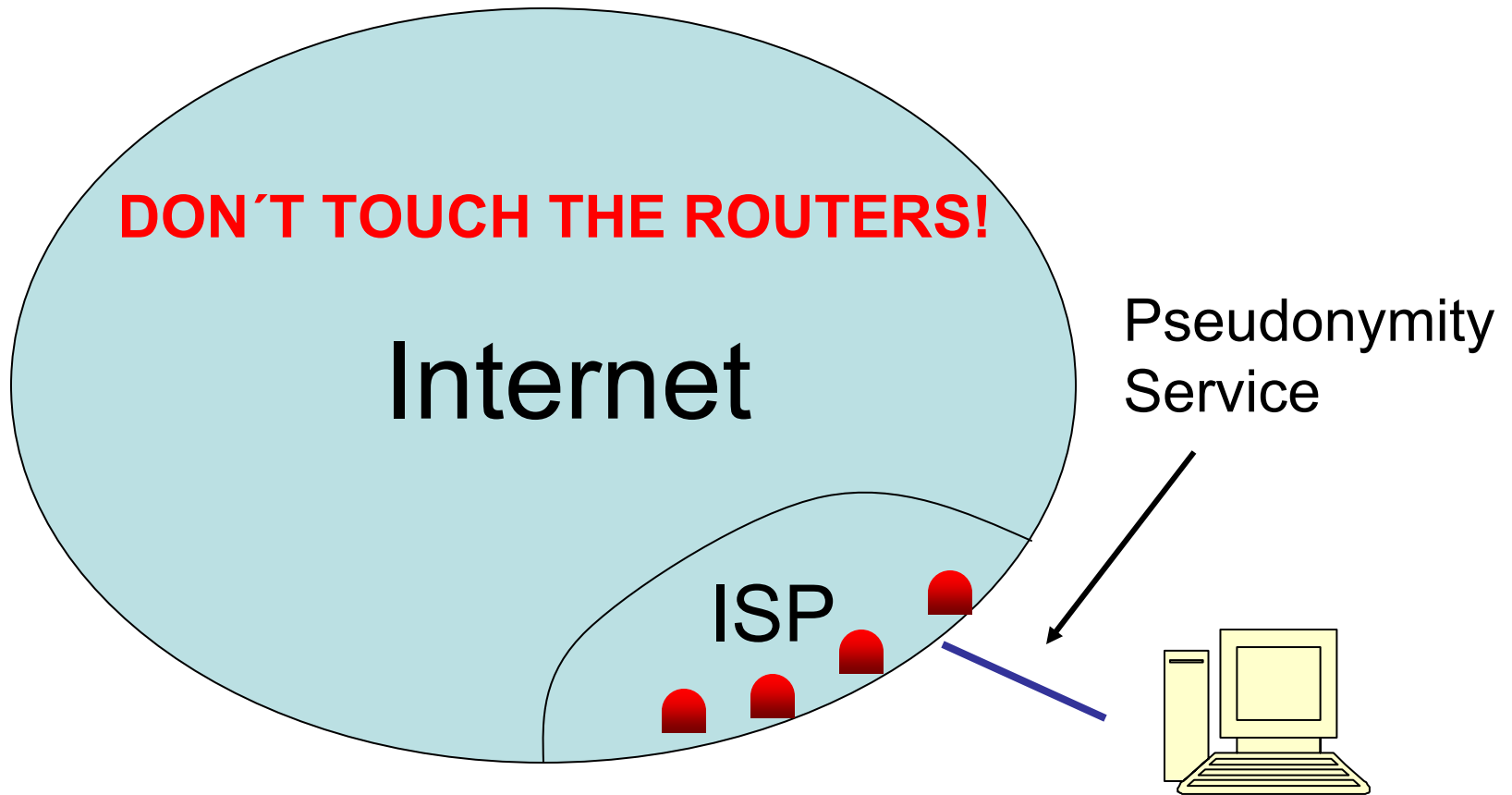


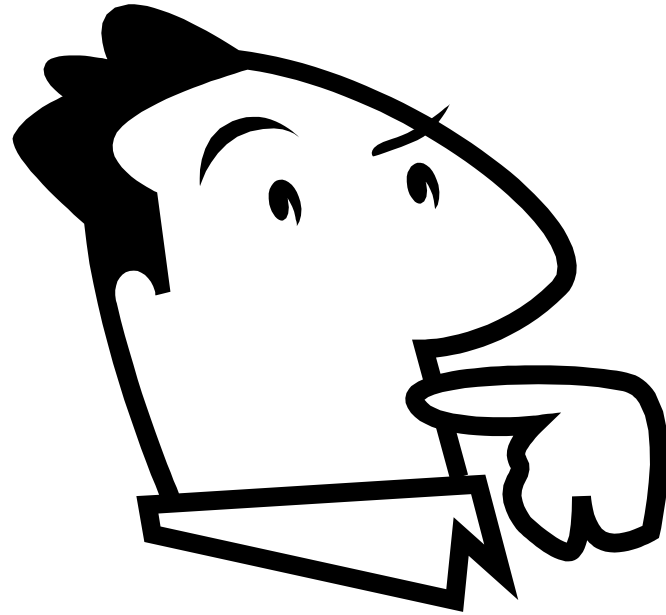
Control over **number** of identities

# Introduction



# Realization





**Questions?**