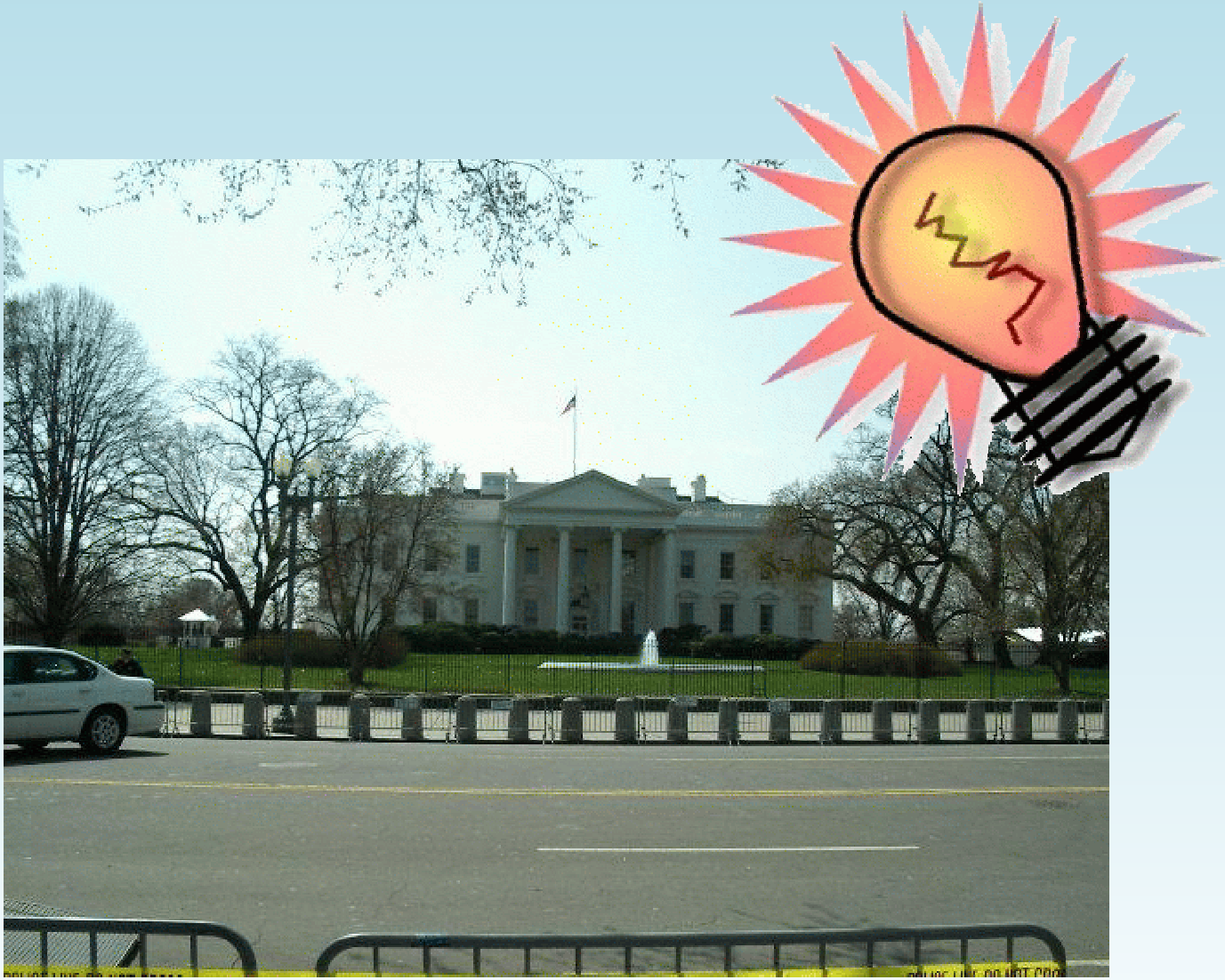
New Intrusion Detection Strategies by the use of Partial Outsourcing

Implemented in the ASCap Framework

Jörg Abendroth

Distributed Systems Group
Trinity College, Dublin

Imagine ...



Presentation Outline

- Levels of Outcourcing
  - Overview of α-,β-,γ-,δ Classes
- The Partial Outsourcing Paradigm
- The ASCap Framework
- Examples of new Intrusion Detection Strategies
  - Advanced Pattern Recognition
  - Active Intruder Recognition
  - Active Probing
- Example Implementations

Class α:Single Administration,Internal

* Administration fully handled by local company

\- Local company requires expertise in all security aspects

\+ No external entity needs to be trusted

Class β:Single Administration,External

* Can also be called "Full Outsourcing"

+ External company provides expertise and manpower

- Local company needs to trust external company (eg. is not malicious, ensures high quality of work, fair after contract finished)

Class γ

Outsourcing via External Security Server

External company provides advice in form of credential, which will be considered in the access control decision function.

Class γ

Outsourcing via External Security Server

External company provides advice in form of credential, which will be considered in the access control decision function.

* Various flavours exist

\+ Local company benefits from outsourcing

\+ Local company does not fully need to trust the external company

Class δ

Partial Outsourcing using External Rule Servers

External company provides help by contributing part of the access control decision function.

Class δ

Partial Outsourcing using External Rule Servers

External company provides help by contributing part of the access control decision function.

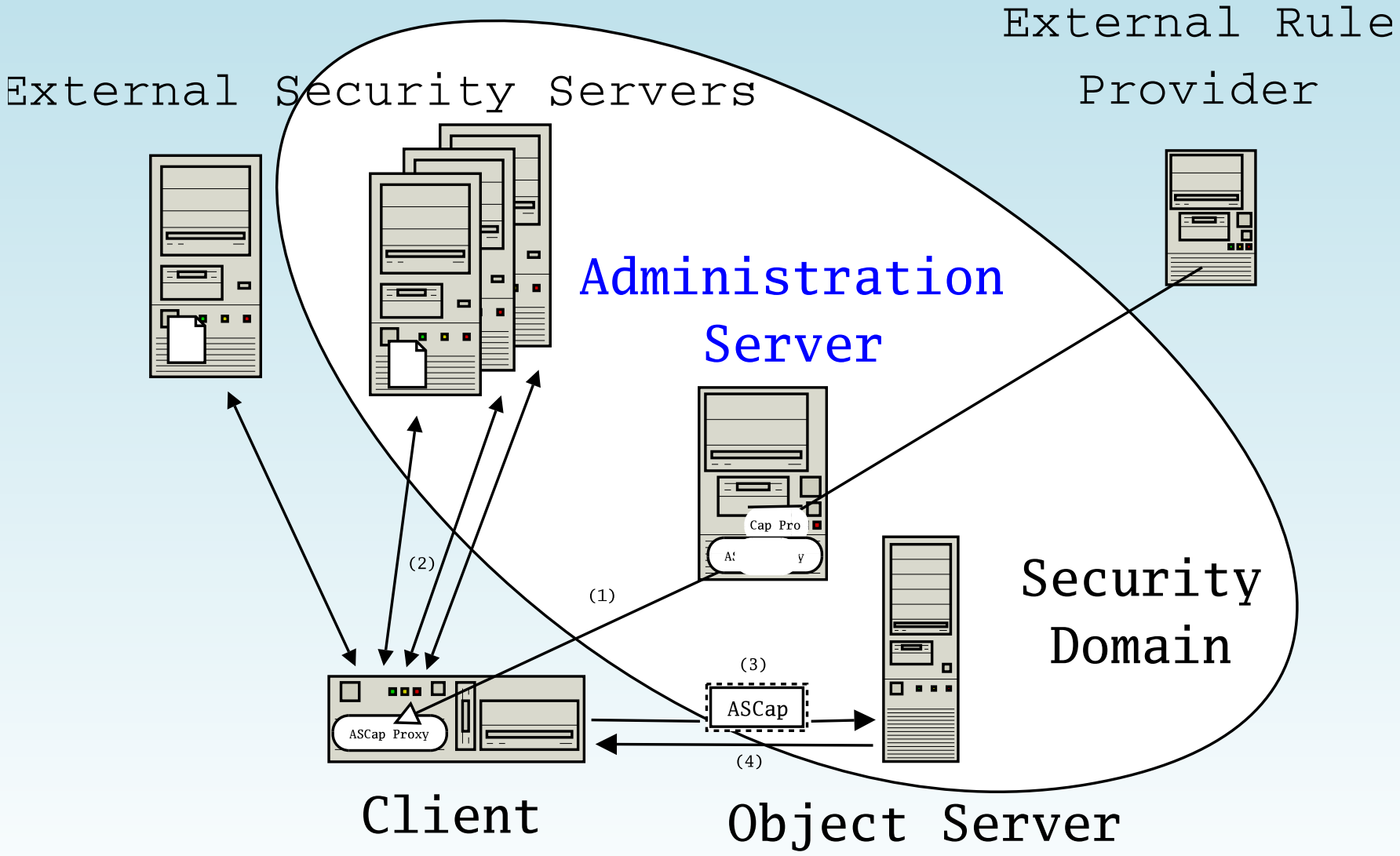
+ Benefits and trust relations similar class γ
+ Enhanced flexibility, because a rule can be any executable code

The Partial Outsourcing Paradigm

Once realized, that access control can not only be "full" or "not" outsourced, but also partially, the **Partial Outsourcing Paradigm** can be written:

> Partial Outsourcing of access control is the method of deciding access by evaluating different rules, which are written by different parties, while the control over the influence each rule can get is left to one party.

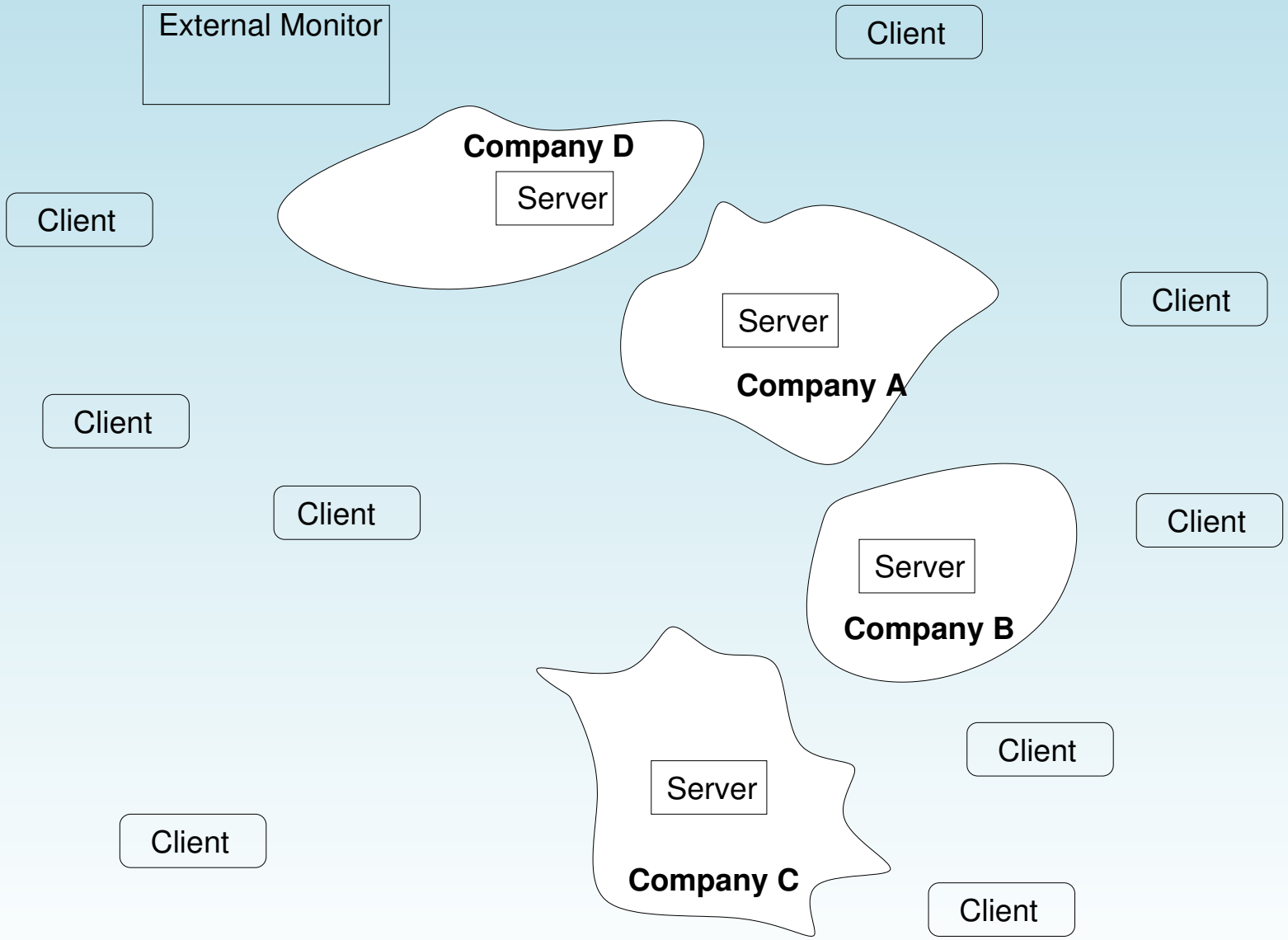
The ASCap Framework



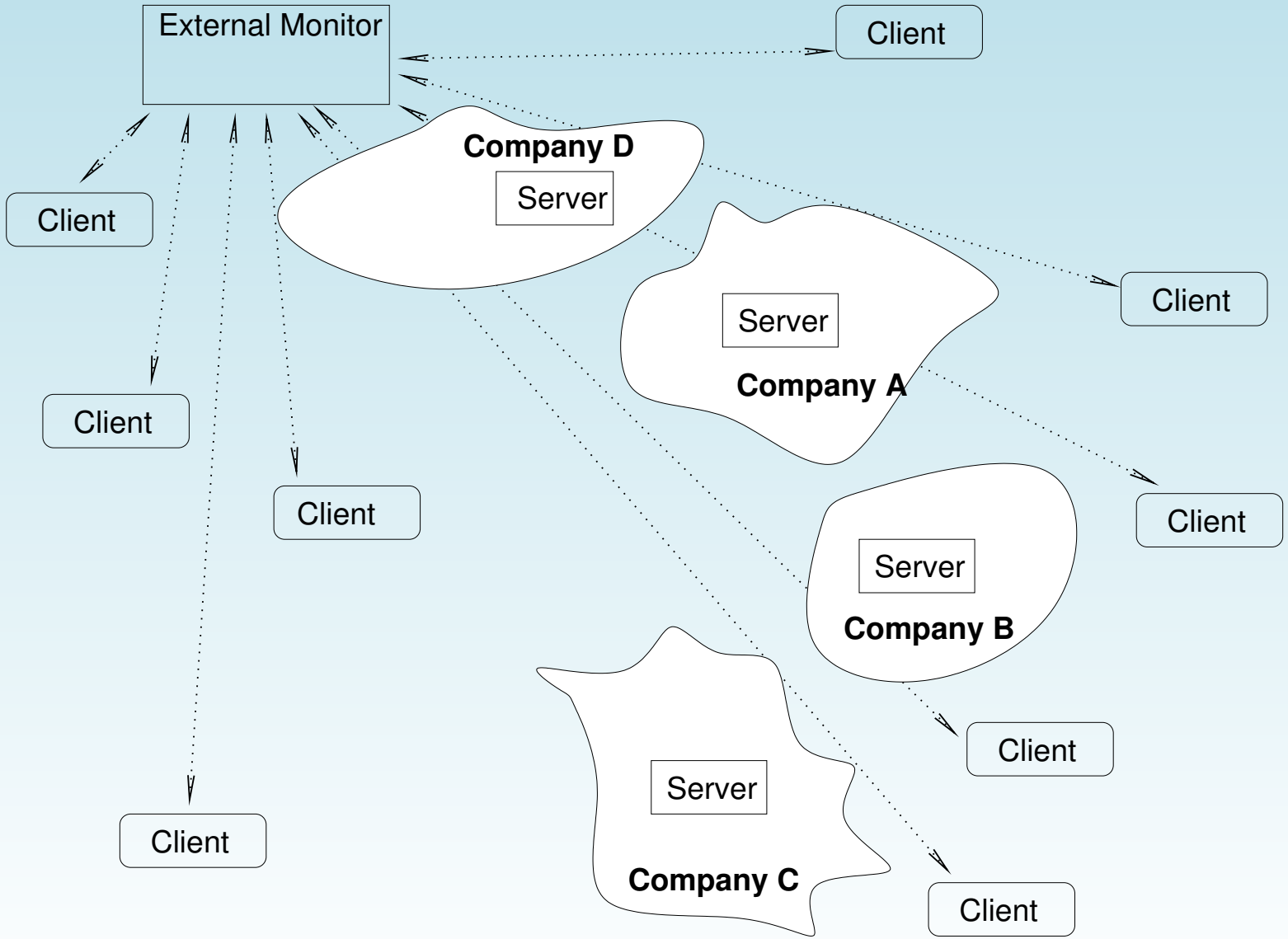
Presentation Outline

- Levels of Outcourcing
  - Overview of α-,β-,γ-,δ Classes
- The Partial Outsourcing Paradigm
- The ASCap Framework
- Examples of new Intrusion Detection Strategies
  - Advanced Pattern Recognition
  - Active Intruder Recognition
  - Active Probing
- Example Implementations

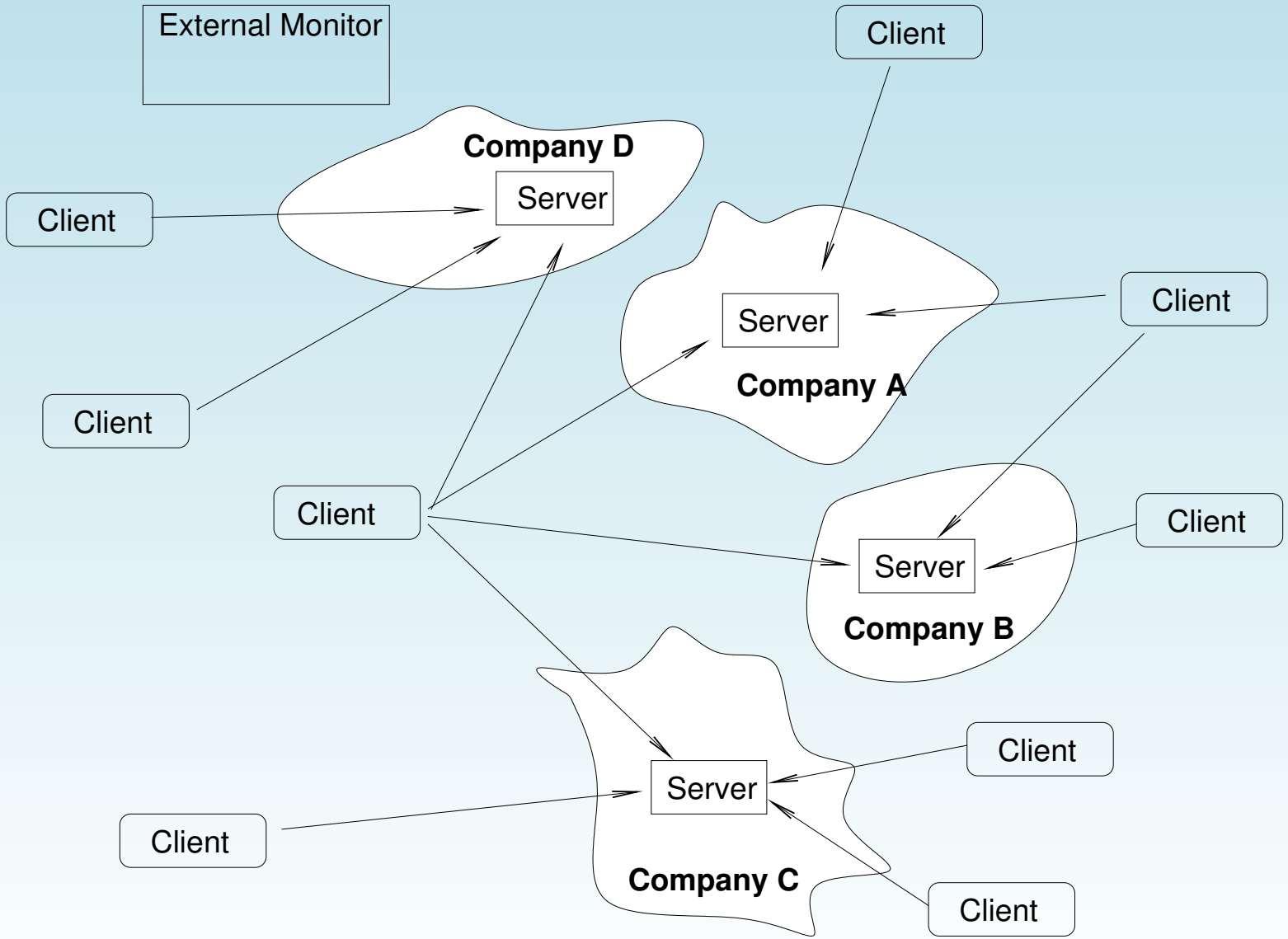
Advanced Pattern Recognition



Advanced Pattern Recognition

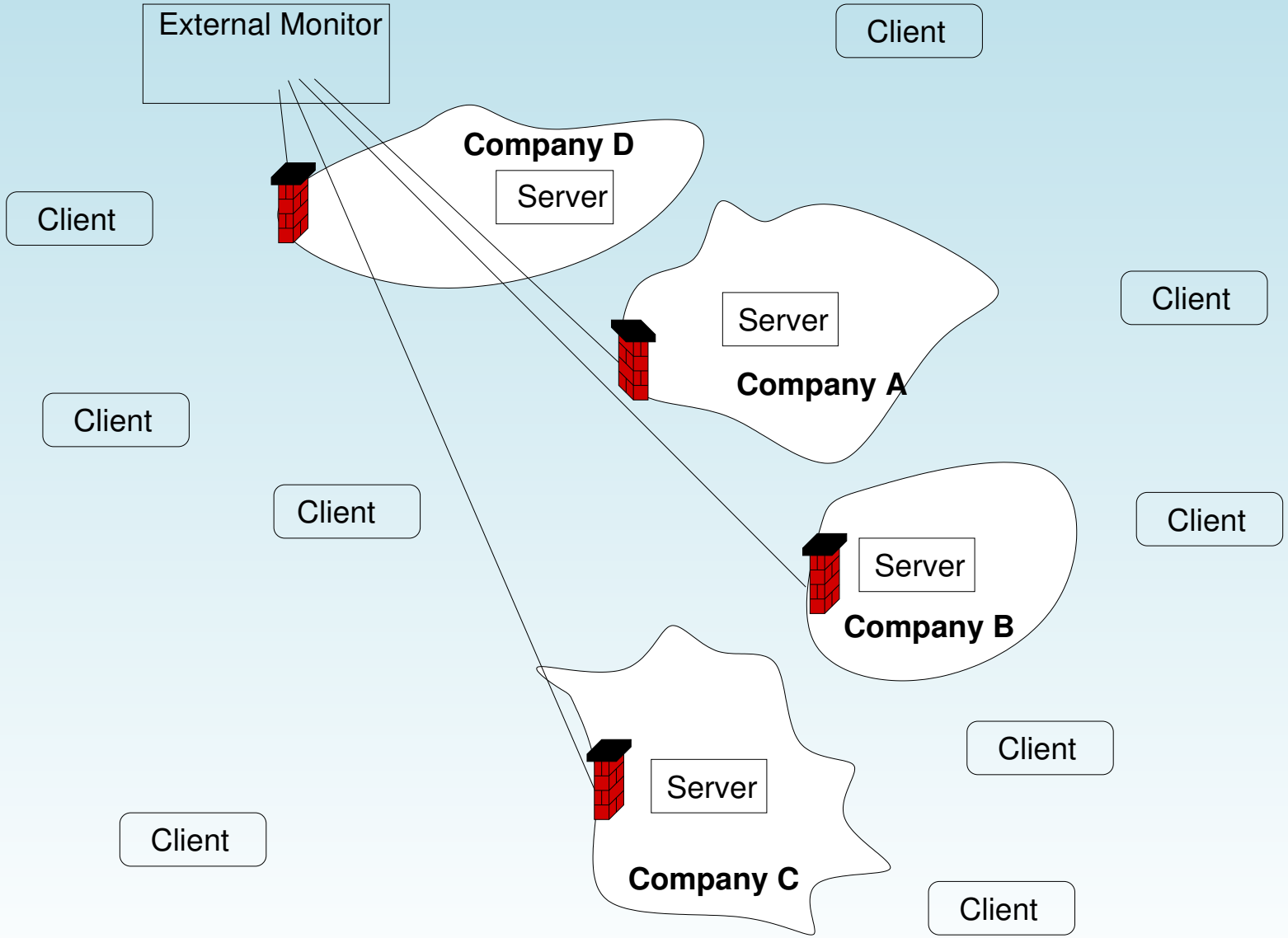


Advanced Pattern Recognition



Advanced Pattern Recognition

(Intrusion Prevention)



Active Intruder Recognition

- High security (i.e. many repeated authentications using different methods) can be cumbersome, but ..

Active Intruder Recognition

- High security (i.e. many repeated authentications using different methods) can be cumbersome, but ..

  High Security made convenient:

  1. Profile the user-system interaction using statistical methods.

Active Intruder Recognition

- High security (i.e. many repeated authentications using different methods) can be cumbersome, but ..

  High Security made convenient:

  1. Profile the user-system interaction using statistical methods.
  2. Periodically switch authentication method (separate statistics!).

Active Intruder Recognition

- High security (i.e. many repeated authentications using different methods) can be cumbersome, but ..

  High Security made convenient:

  1. Profile the user-system interaction using statistical methods.
  2. Periodically switch authentication method (separate statistics!).
  3. If statistics differ -> investigate.

Active Intruder Recognition

- High security (i.e. many repeated authentications using different methods) can be cumbersome, but .. using dynamically changing environments can be achieved conveniently.
- Environment changes give an opportunity to unveil certain attacks, such as the playback attack.

Active Probing

- Active probing employs interdisciplinary results of e.g. criminological profiling.
- Predicted properties of intruders are used to create a test.
- Active probing tests allow to reveal intruders otherwise hidden.
- Partial outsourcing provides infrastructure required to employ active probing tests.

Example Implementations

Example	Class	Ext. Sec. Server	Ext. Rulel Server	Comment (Tested?)
Advanced Pattern Recog.	γ	x	-	External security server stops handing out credentials if extensive access rigths are detected ($\surd$)
Active Intruder Recog. 1	δ	-	x	Policy changes regularly and statistics about access requests are compared. ($\surd$)
Active Intruder Recog. 2	δ	-	x	IDS alarm causes system to switch to policy P_{alarm}. If statistics of the next hour do not differ from normal state, the system goes back to P_{normal} ($\surd$)
Active Probing	γ	x	x	Using policy changes and ext. sec. server intruder tests are implemented. (-)

Thanks for your Attention !!!

Joerg@Abendroth.info

Research Interests: Access Control Frameworks, Network & Communication System Security

2000 Diplomarbeit Telekom FH-Dieburg:
'Performance of VoIP Channels Over WLans'
2003 Marie Curie Fellowship BRICS, Denmark
2004 PhD Trinity College Dublin
'A unified Access Control Mechanism'