

Automatisierter Identitätsdiebstahl in sozialen Netzwerken

Dominik Birk - Felix Gröbert - Dr. Christoph Wegener

D * A * CH Security 2009
Bochum, 20. Mai 2009



hgi

Horst-Görtz Institut ■
für IT Sicherheit ■

Mitwirkende



Dominik Birk
Mitarbeiter am Horst Görtz Institut für IT-Sicherheit (HGI)



Felix Gröbert
IT Freiberufler

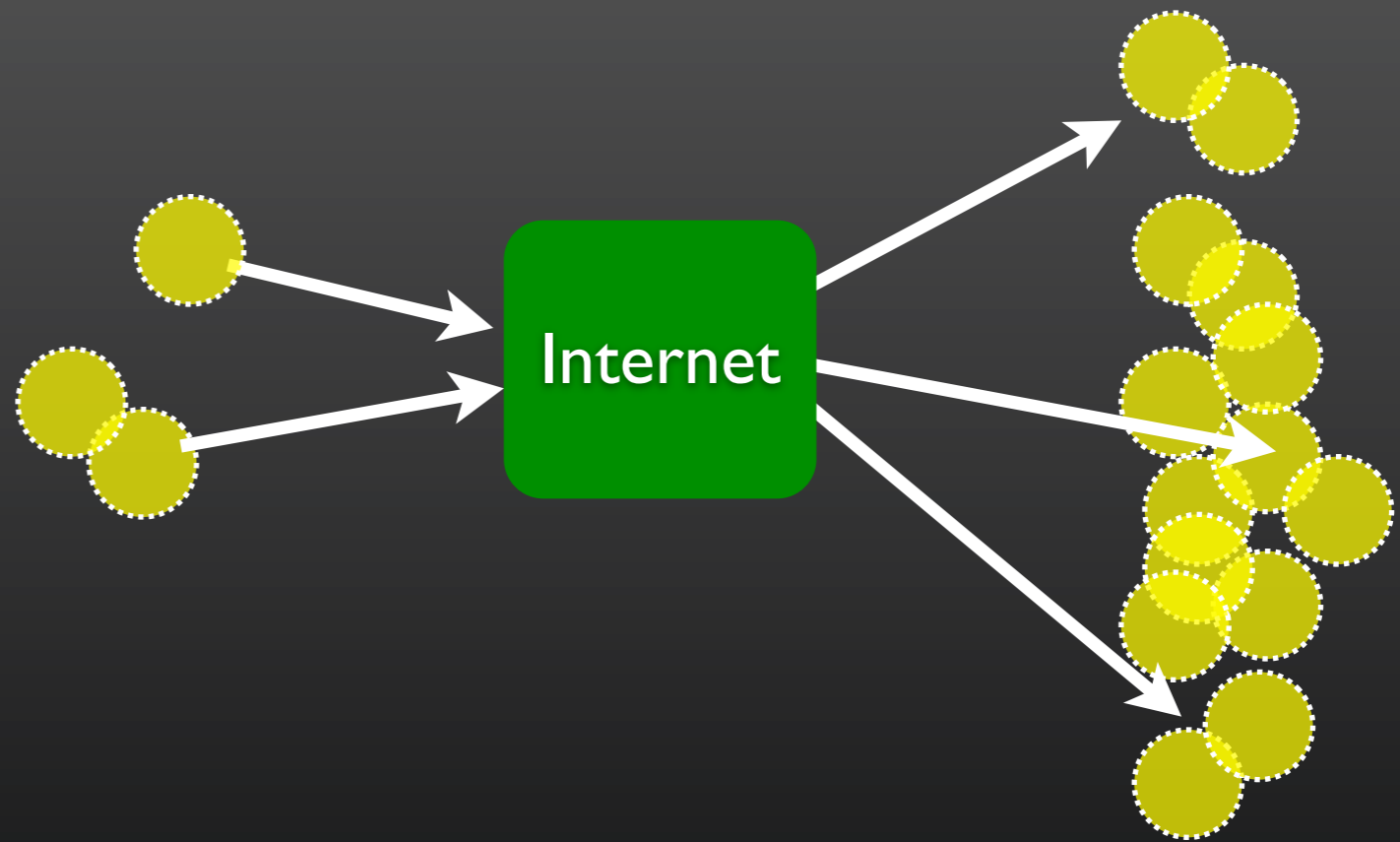


Dr. Christoph Wegener
Mitarbeiter am Horst Görtz Institut für IT-Sicherheit (HGI)

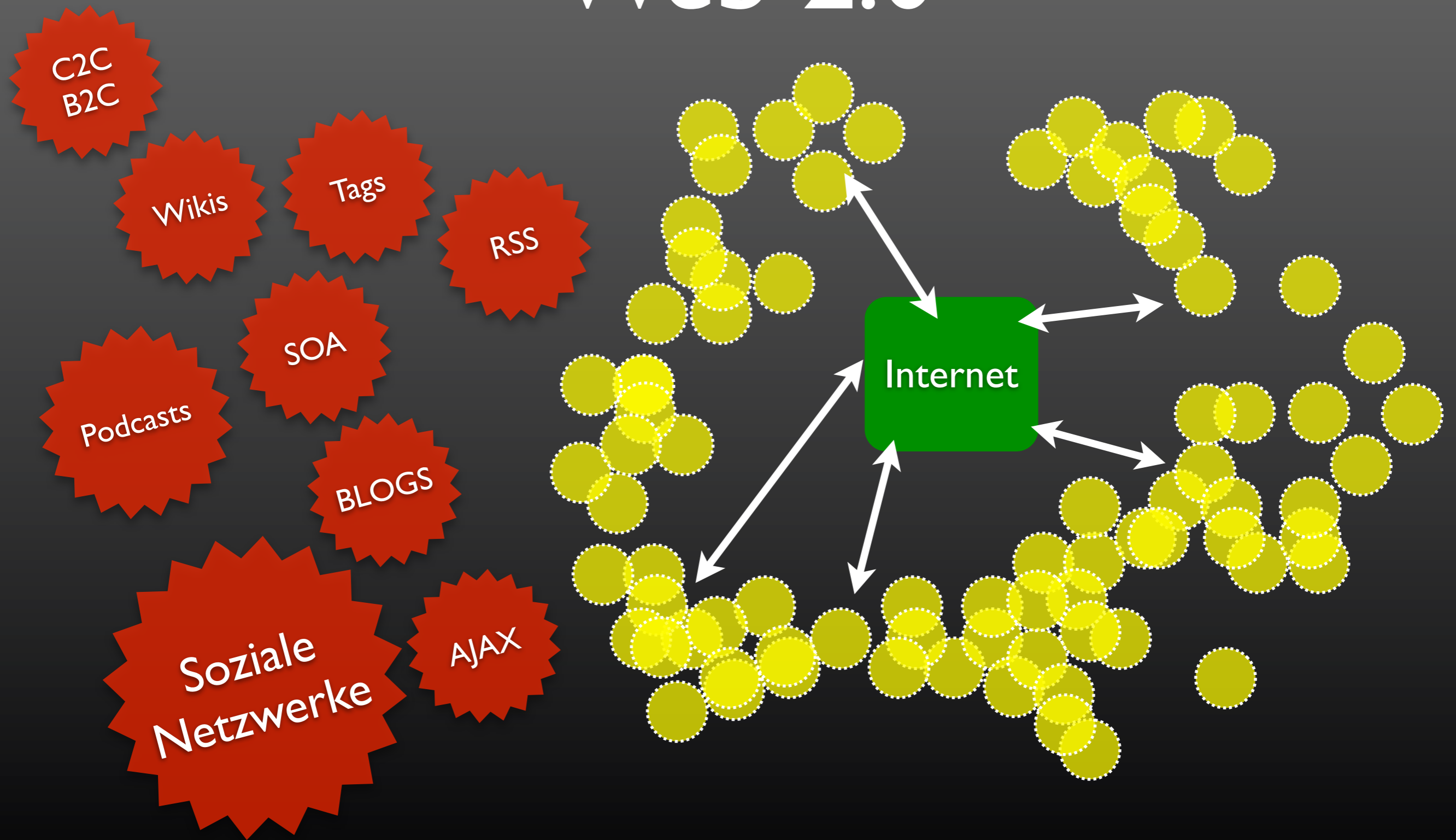
Web 1.0

E-Mail

B2C
E-Commerce



Web 2.0



Wert von Informationen

| Information | Preis in US\$ |
|------------------------------|---------------|
| Internetbanking Zugang | 10–1000 |
| Kreditkarten mit CCV2 | 0,50–12 |
| Kreditkarten | 0,10–25 |
| E-Mail Adressen | ca. 0,35 / MB |
| komplette Identitäten | 0,90–25 |
| Cash-out Service | 8-50% share |
| Proxy | 0,30–20 |
| angepasster Banking-Trojaner | 1000 |

Quellen: Panda Labs - The Business of Cybercrime, Symantec Report on the Underground Economy

Soziale Netzwerke



Soziale Netzwerke



23

66

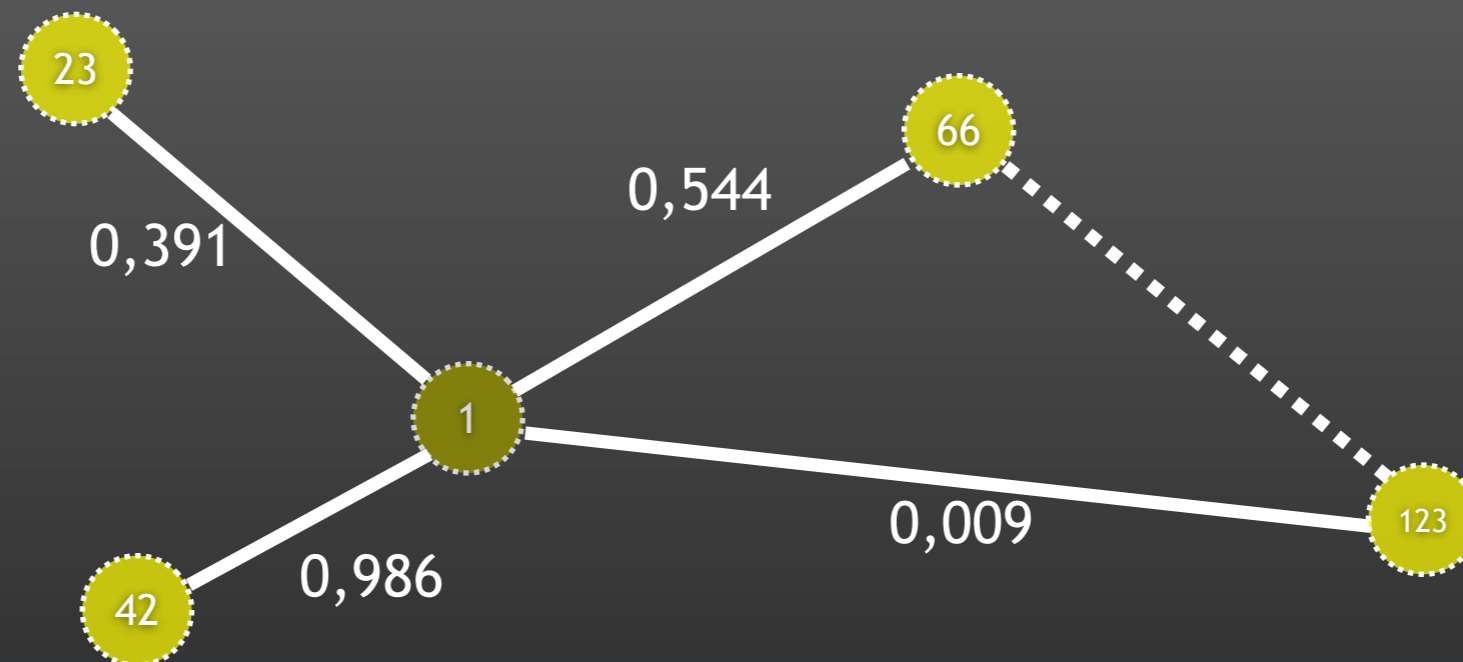
1

123

42

| i_n | 23 | 42 | 66 | 123 |
|-------|----|----|----|-----|
| | | | | |

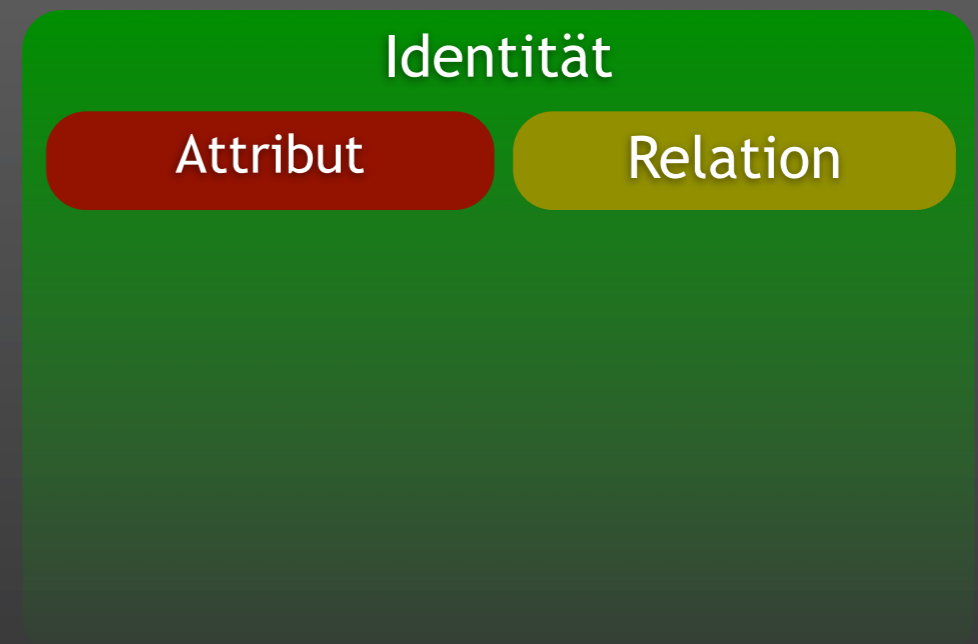
Soziale Netzwerke



| | | | | |
|-------|-------|-------|-------|-------|
| i_n | 23 | 42 | 66 | 123 |
| w_n | 0,391 | 0,986 | 0,544 | 0,009 |

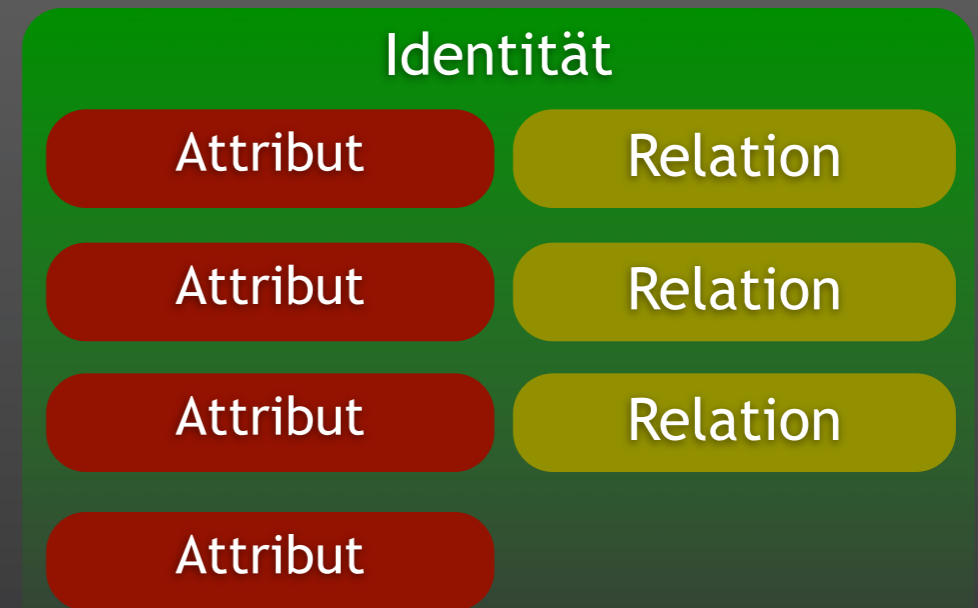
Identitäten

- $(i, A, R) = 3\text{-Tupel}$ zur Beschreibung einer Identität



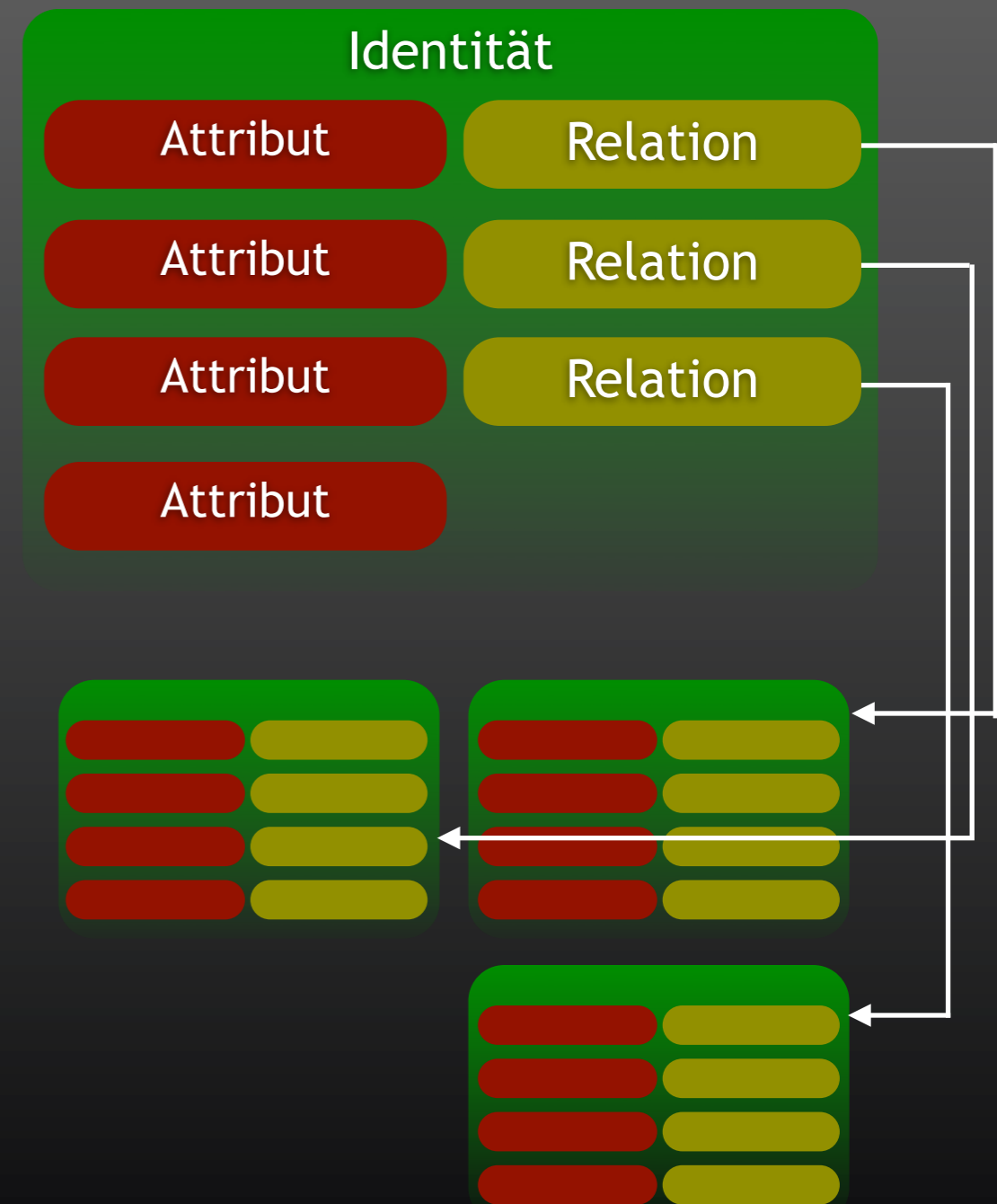
Identitäten

- $(i, A, R) = 3$ -Tupel zur Beschreibung einer Identität
- Attribute:
Name, Adresse, Hobbys,
Geburtsdatum, E-Mail,
Arbeitgeber, CV,
Mitgliedschaften



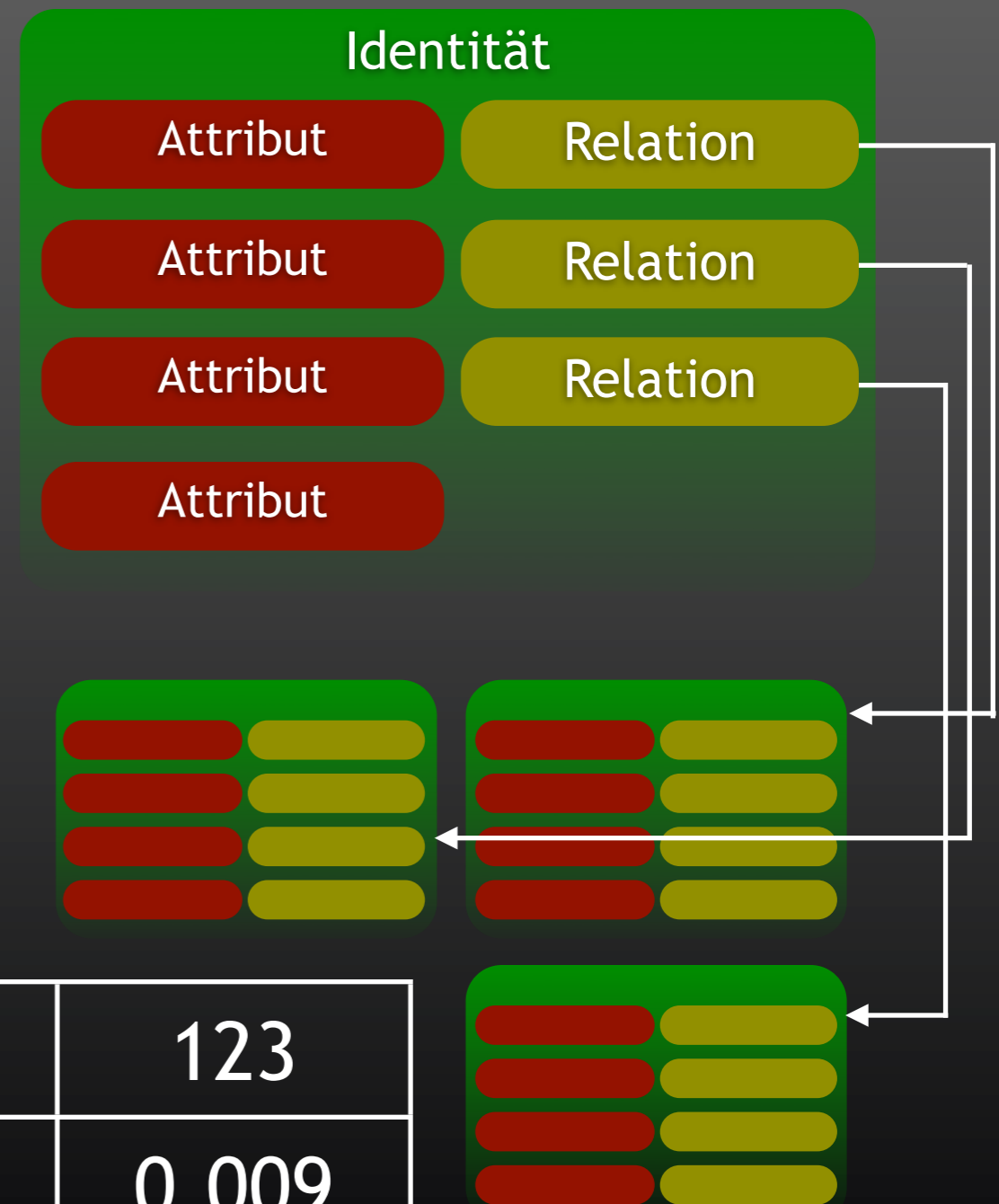
Identitäten

- $(i, A, R) = 3\text{-Tupel zur Beschreibung einer Identität}$
- Attribute:
Name, Adresse, Hobbys,
Geburtsdatum, E-Mail,
Arbeitgeber, CV,
Mitgliedschaften



Identitäten

- $(i, A, R) = 3$ -Tupel zur Beschreibung einer Identität
- Attribute:
Name, Adresse, Hobbys, Geburtsdatum, E-Mail, Arbeitgeber, CV, Mitgliedschaften
- Relationen:



| | | | | |
|-------|-------|-------|-------|-------|
| i_n | 23 | 42 | 66 | 123 |
| w_n | 0,391 | 0,986 | 0,544 | 0,009 |

Ziele des Angreifers

- Automatische Aggregation von Nutzerprofilen sozialer Netzwerke
- Möglichst viel Informationen über potentielle Opfer
- $\text{deg}(a, r) := \sum a + \sum r$
- Identitäts-Korrelation
- Daten-Analyse
- Angriff: Fortgeschrittener Identitätsdiebstahl



Ziele des Angreifers

- Automatische **1. Aggregation** von Nutzerprofilen sozialer Netzwerke
- Möglichst viel Informationen über potentielle Opfer
- $\text{deg}(a, r) := \sum a + \sum r$
- Identitäts- **2. Korrelation**
- Daten- **3. Analyse**
- **4. Angriff**: Fortgeschrittener Identitätsdiebstahl

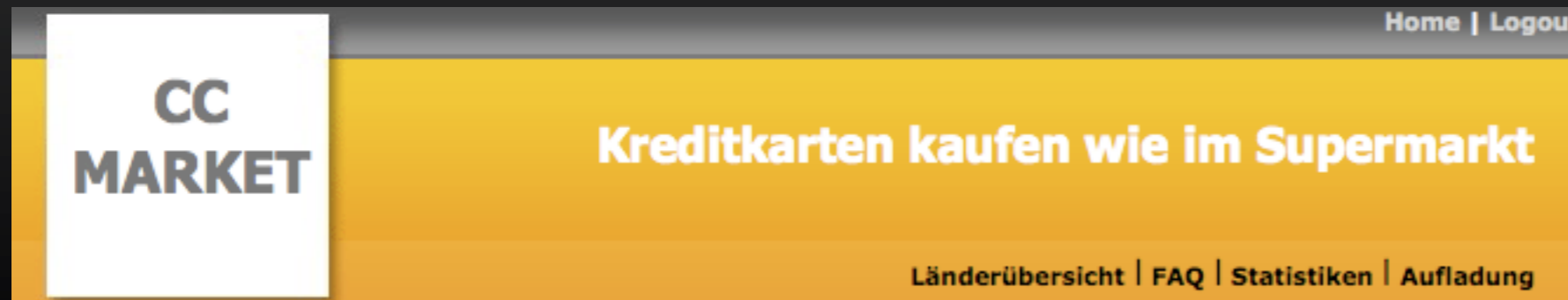


Trade-Off

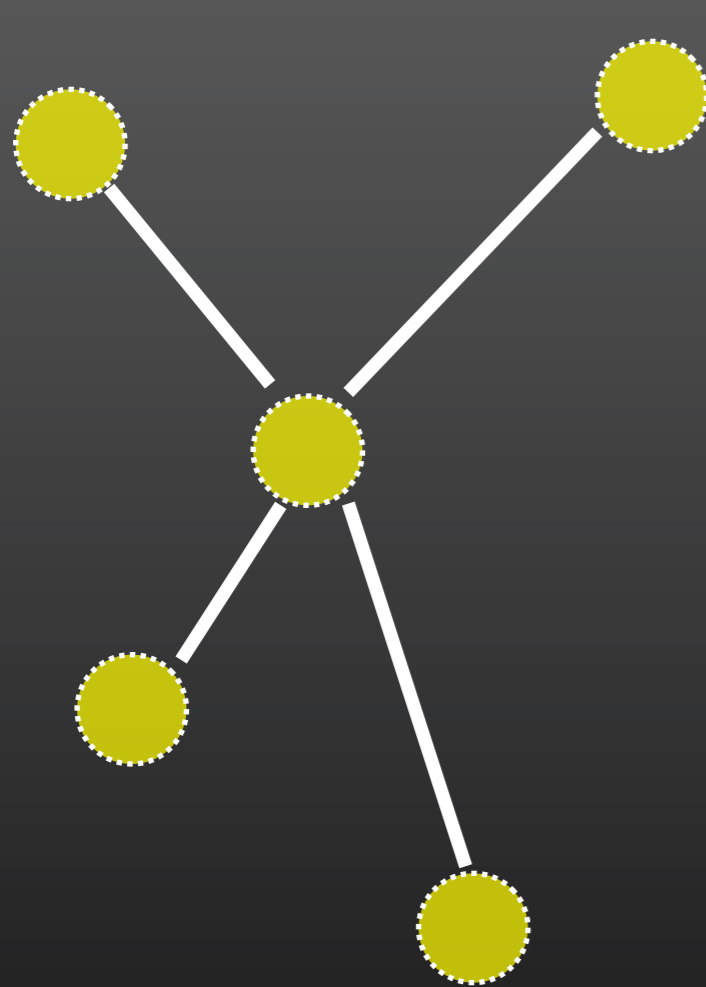


Aggregation

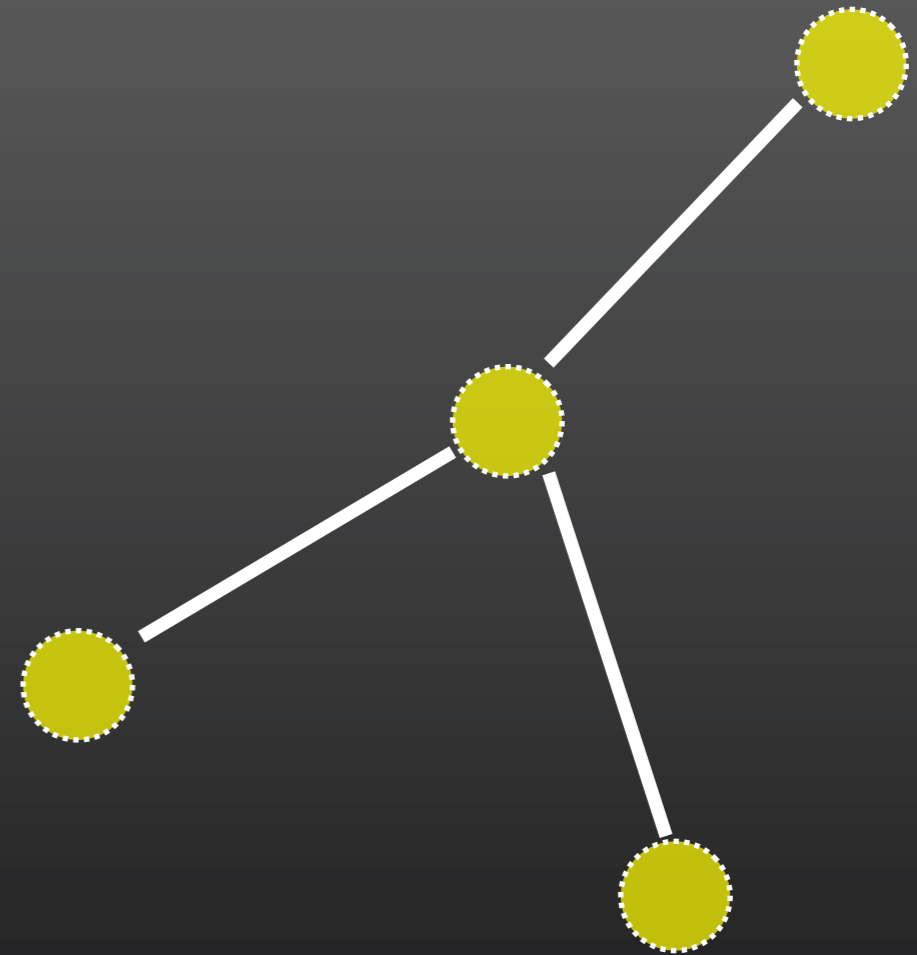
- *Crawling*: Simulation von Nutzerverhalten
- Wird meist durch einheitliche Darstellung & Struktur vereinfacht
- *Cracking*: Im Zeitraum vom 1.1. bis 29.7.08: 25118409 personenbezogene Daten gestohlen
- *Buying*: illegal - Foren, IM, IRC; legal - Datenhändler, Call Center, Meldeämter



Korrelation

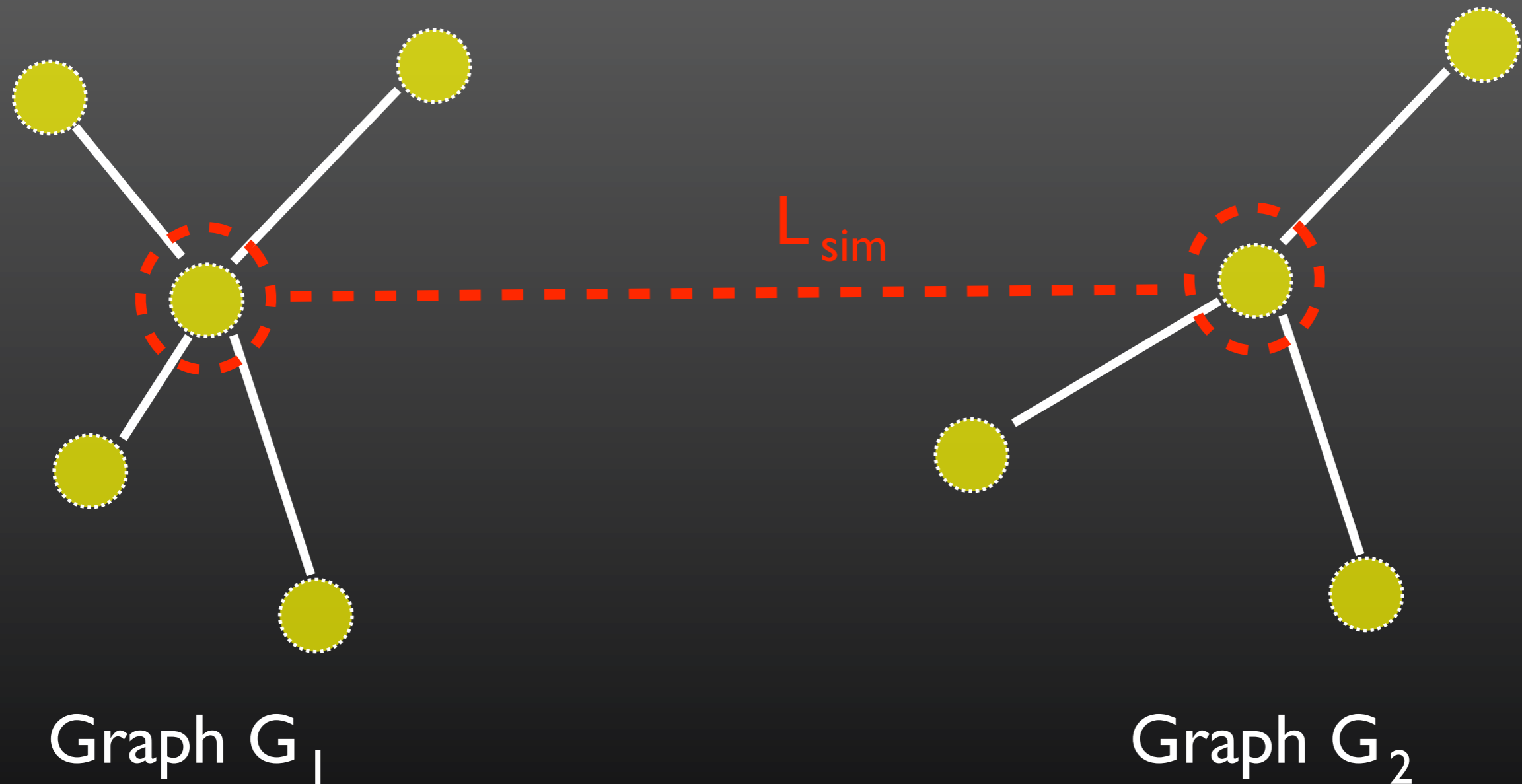


Graph G_1

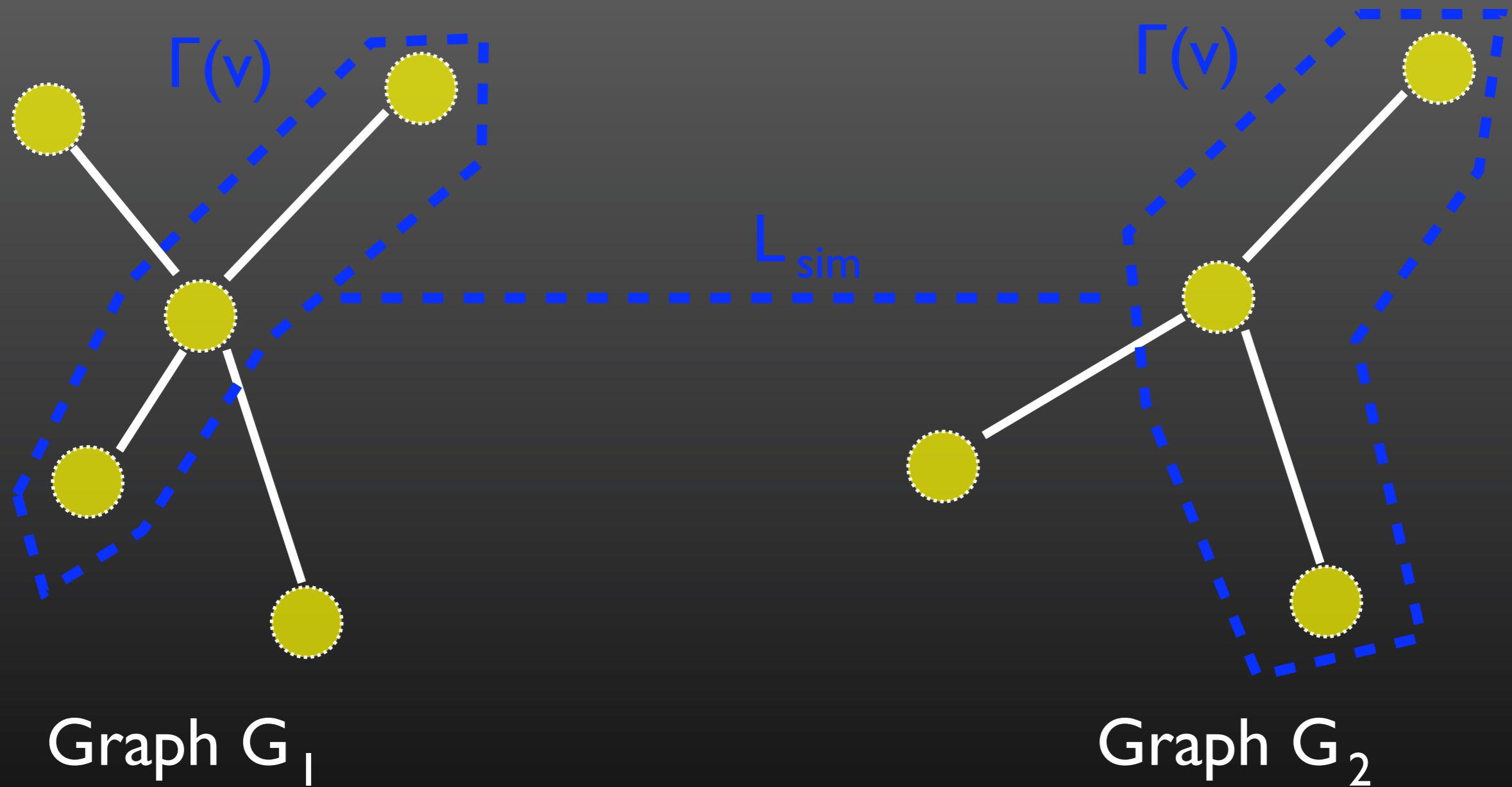


Graph G_2

Korrelation



Korrelation



Korrelation

- Untersuchung der *Nachbarschaft* eines Zielknotens
- Graphen-basiertes Data-Mining
- Topologische Struktur: Algorithmus für Sub-Graph Isomorphismus (*NAUTY*)

Ist Graph G_1 isomorph zu einem Subgraphen von G_2 ?

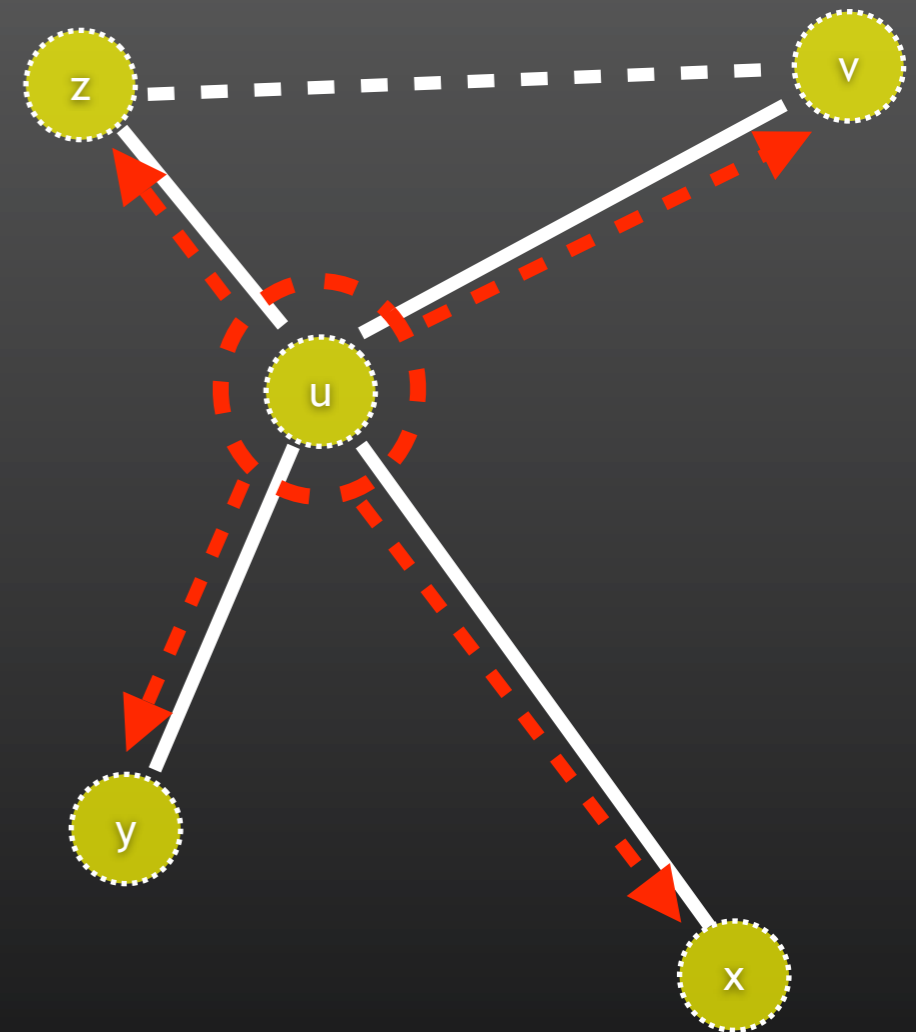
- Wenn $L_{\text{sim}} > \text{Grenzwert } \pi$, Profilervollständigung möglich

Daten-Analyse bzw. Opferwahl

- Maximales Informationsgehalt über Identität verfügbar?
 $\text{deg}(a,r) \rightarrow \max$
- Existiert ein *Broker* im Sub-Graph?
- Existiert eine *Clique* (vollständiger Sub-Graph)?
- Maximaler Cluster-Koeffizient? (impliziert ausgeprägte *Nachbarschaft*)

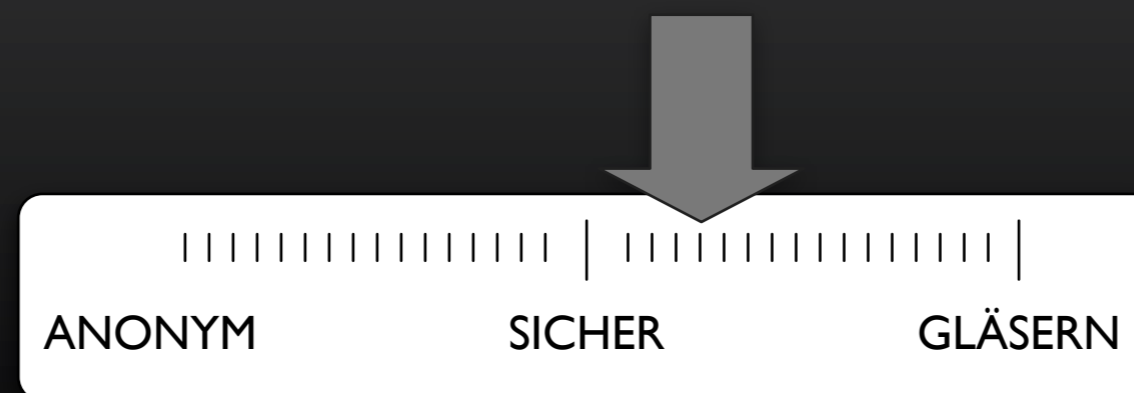
Angriff

- Missbrauch der Vertrauensbeziehung unter den Nutzern
- Vorherige Phasen helfen bei Auswahl geeigneter Opfer
- Missbrauch öffentlicher, persönlicher Attribute
- „Hallo [v, x, y, z], ich bins u“

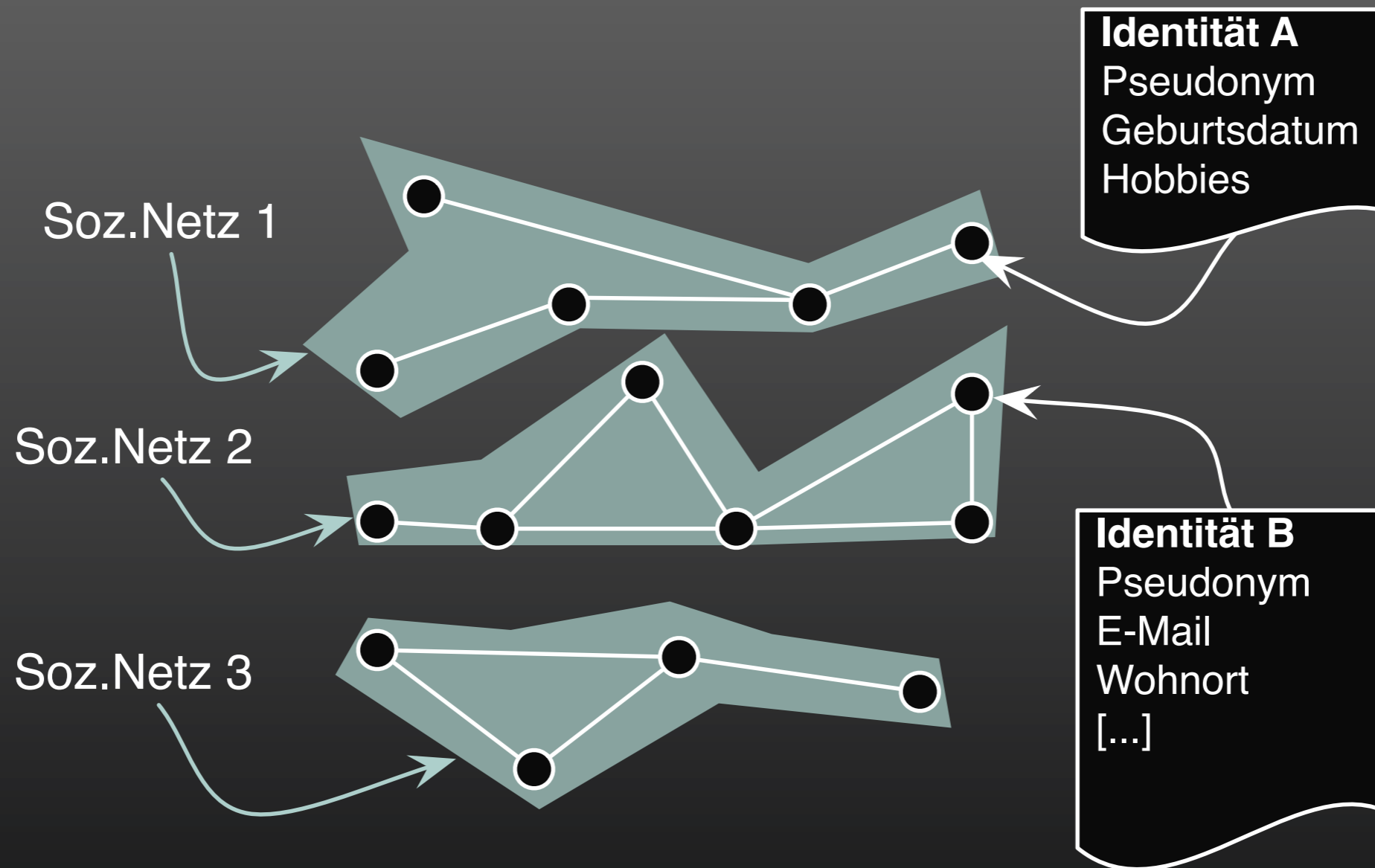


Gegenmaßnahmen

- Pseudonymisierung der Benutzerkonten
- Anti-Crawling Maßnahmen durch den Anbieter
- Verbesserung der Applikations-Sicherheit
- Bewusstsein für Datensparsamkeit schärfen
- Datenschutzmöglichkeiten der Anbieter nutzen

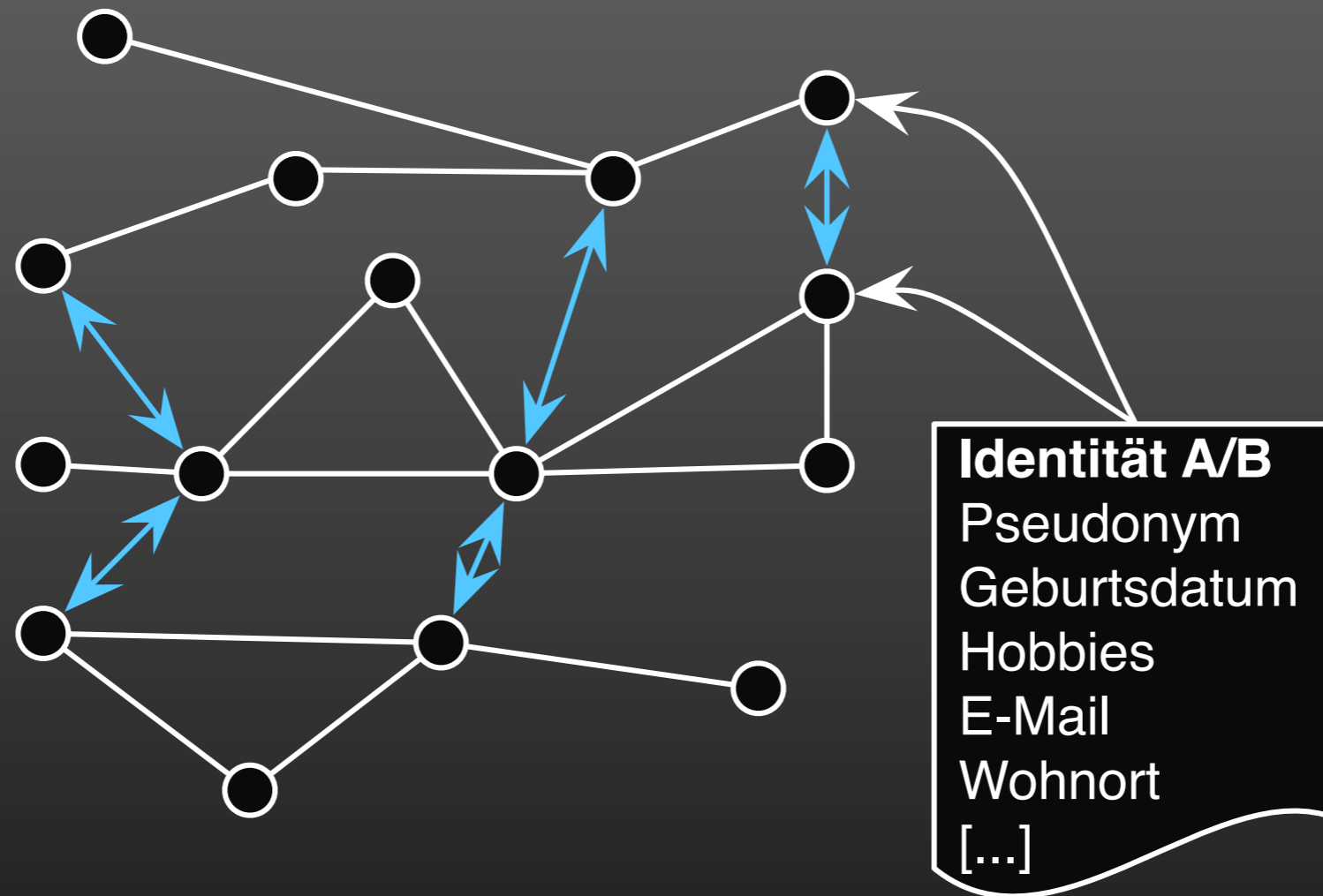


Überblick



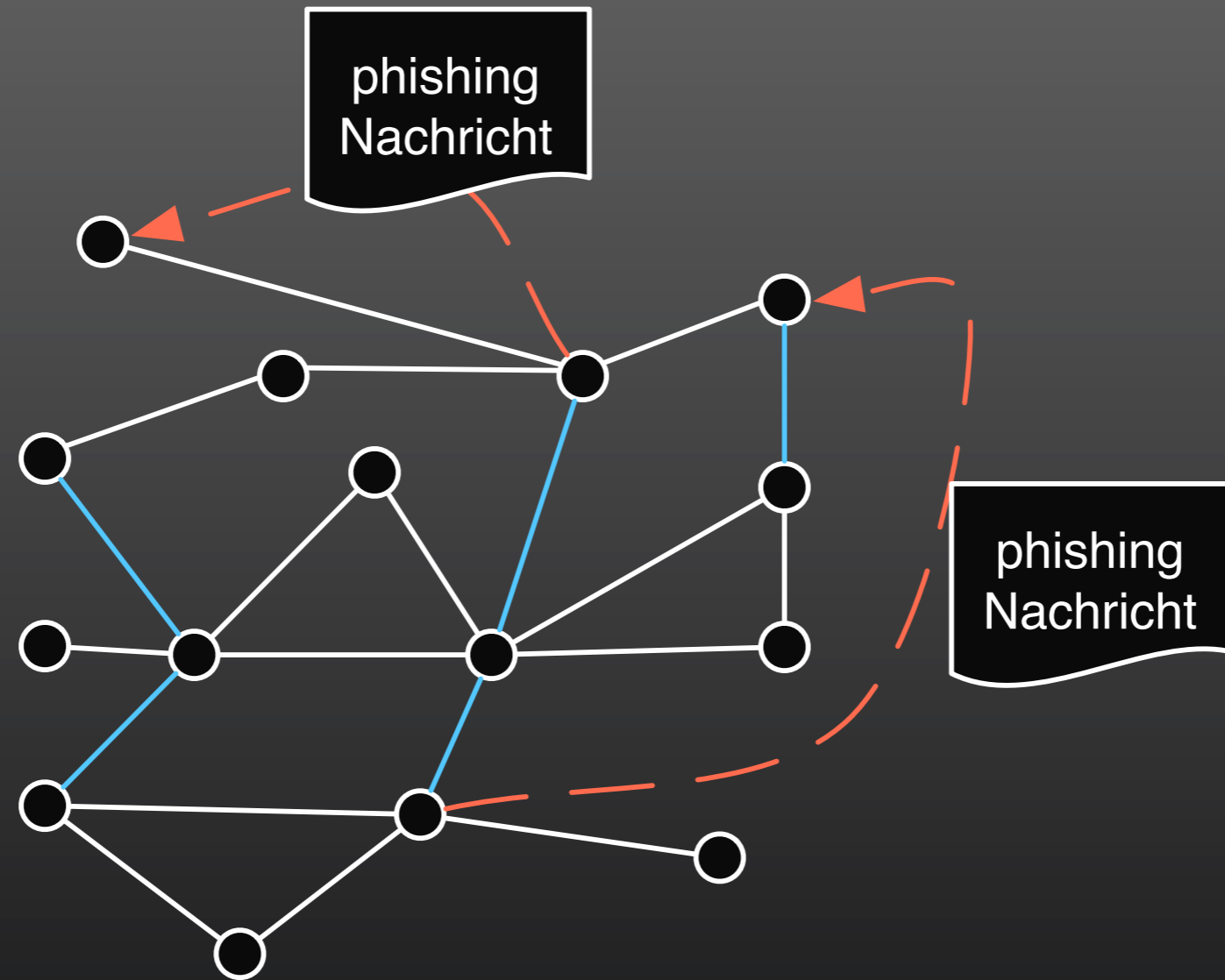
Aggregationsphase

Überblick



Korrelationsphase

Überblick



Angriffsphase

Fazit

- Soziale Medien leben von personenbezogenen Daten
- Erbeuten & Korrelieren von personenbezogenen Daten leicht möglich
- Bewusstsein für Datensparsamkeit nicht ausreichend ausgebildet
- Schutz von Daten ist auch Pflicht der Anbieter
- Web-2.0 bietet enormes Missbrauchspotential



Vielen Dank für Ihre Aufmerksamkeit!
Fragen oder Anmerkungen?

dominik@code-foundation.de
felix@groebert.org
wegener@wecon.net