Karlsruhe Institute of Technology

Reduktion einer RBAC-Instanz
Basierend auf Ansätzen der Graphentheorie

Access Control Lab: Abschlusspräsentation
Jean-Marc Hendrikse

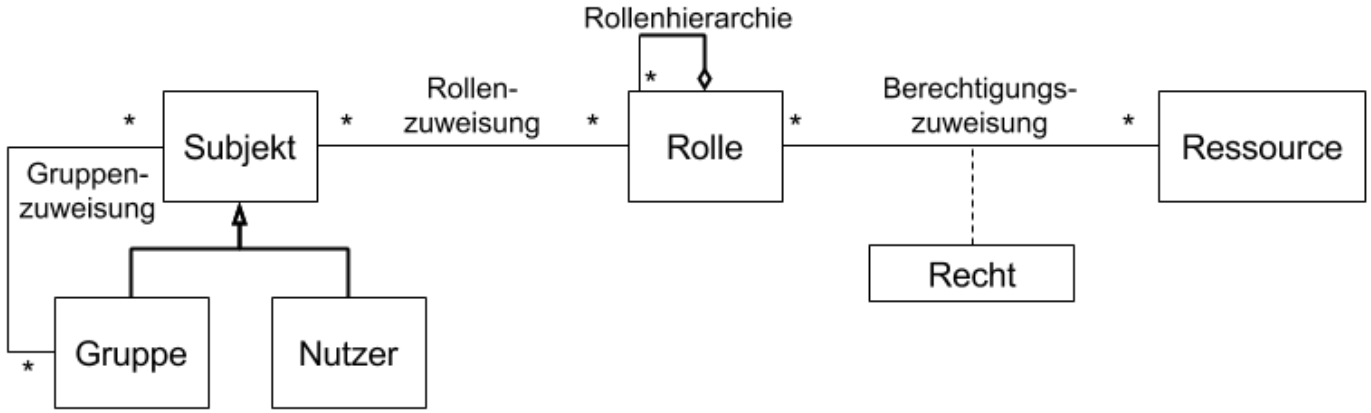
DECENTRALIZED SYSTEMS AND NETWORK SERVICES RESEARCH GROUP (DSN)
INSTITUTE OF TELEMATICS, FACULTY OF INFORMATICS


```c
/*
 * Playground module for the LSM framework.
 *
 */

#define pr_fmt(fmt) "ACS-Lab: " fmt

#include <linux/lsm_hooks.h>
#include <linux/time64.h>   // timespec64
#include <linux/time.h>     // ktime_get
#include <linux/path.h>     // path
#include <linux/dcache.h>   // dentry_path
#include <linux/string.h>   // strncmp
#include <linux/usb.h>      // USB

/*** Hook handler definitions ***/

#define VENDOR_ID 0x0000
#define PRODUCT_ID 0x0000

static int match_usb_dev(struct usb_device *dev, void *unused)
{
    return ((dev->descriptor.idVendor == VENDOR_ID) &&
        (dev->descriptor.idProduct == PRODUCT_ID));
}
```

```c
    char *ret_path;

    ret_dir = dentry_path(dir->dentry, buf_dir, ARRAY_SIZE(buf_dir));
    if (IS_ERR(ret_dir)) {
        pr_info("mkdir hooked: <failed to retrieve directory>\n");
        return 0;
    }
    ret_path = dentry_path(dentry, buf_path, ARRAY_SIZE(buf_path));
    if (IS_ERR(ret_path)) {
        pr_info("mkdir hooked: <failed to retrieve path>\n");
        return 0;
    }
    pr_info("mkdir hooked: %s in %s\n", ret_path, ret_dir);
    // Add your code here //

    return 0;
}


static int acslab_settime (const struct timespec64 *ts, const struct timezone *tz)
{
    pr_info("settime hooked\n");
    return 0;
```

Aufgabenbeschreibung und Problemstellung

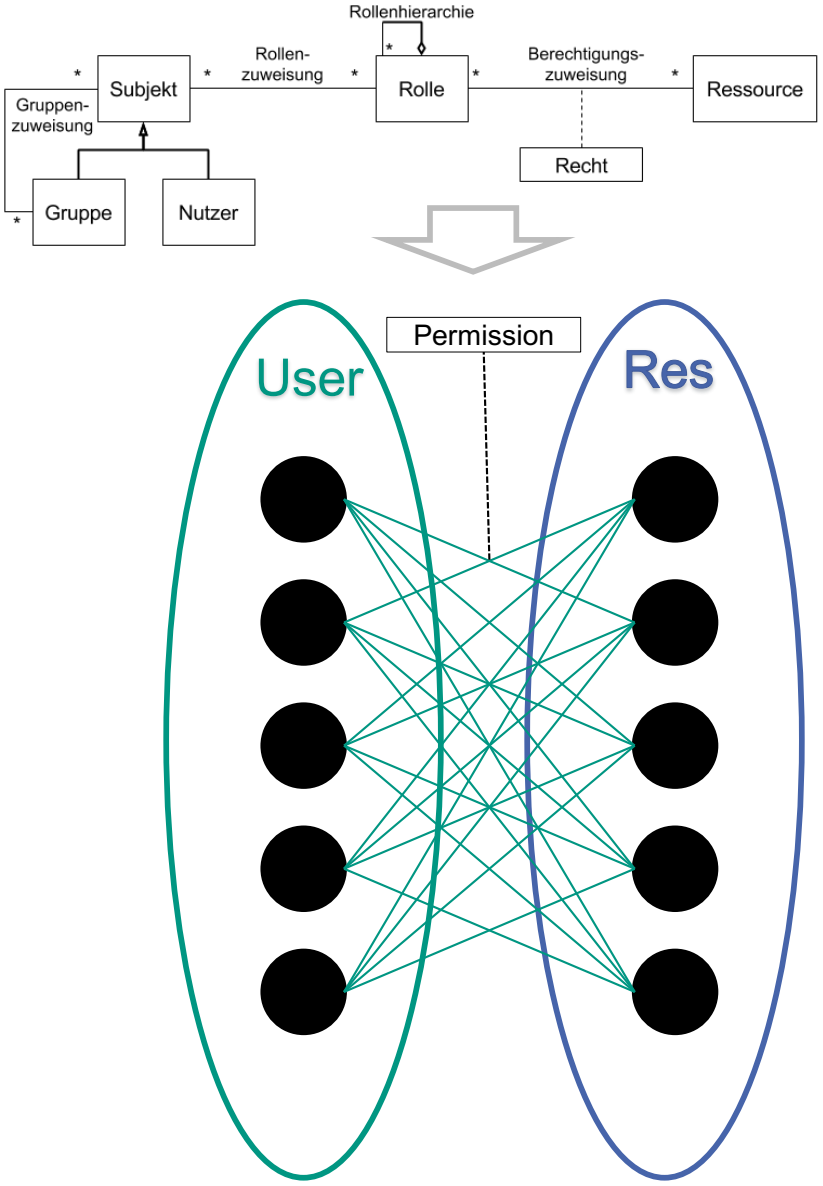
- Role-Based Access Control (RBAC) ist ein sehr häufig eingesetztes Autorisierungs- und Zugriffsmodell
- Rollen repräsentieren Rechte und Pflichten einer spezifischen Aufgabenbeschreibung (beispielsweise in einem Unternehmen)
  - Besonders für sehr große Unternehmen (mit tausenden von Mitarbeitern) wird der Entwurf von Rollen sehr komplex
  - Häufig: Rollenzuweisungen nicht aktuell, Rollen redundant, Suboptimale Rollenzuweisungen
- Praktikumsaufgabe: Reduzierung von Rollen und Rechtezuweisungen einer gegeben RBAC-Instanz



DSN Research Group
Institute of Telematics, Faculty of Informatics

Das Role-Mining-Problem (RMP)

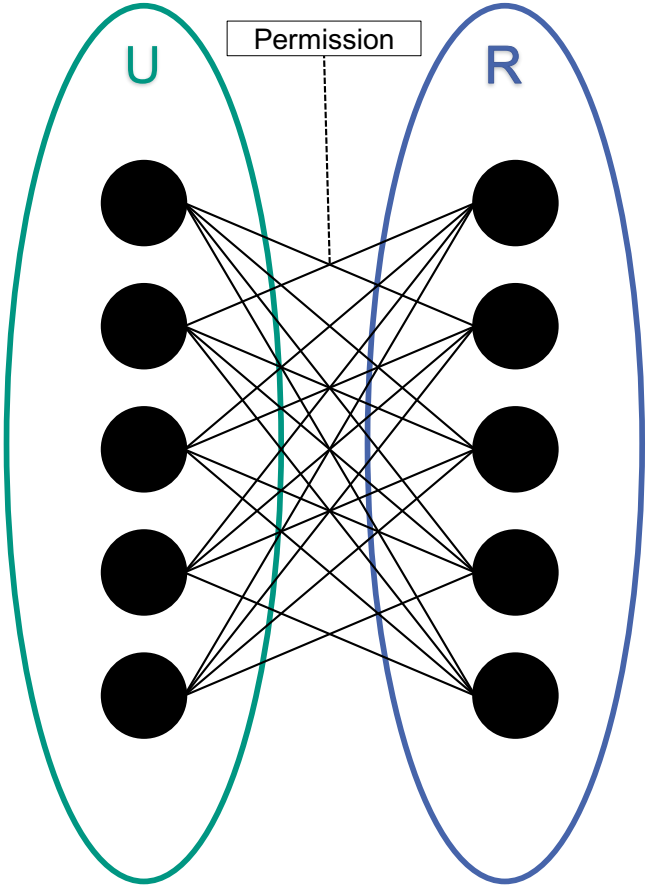
- Ansatz äquivalent zu: Finden einer minimalen Bicliquen-Überdeckung (NP-Schwer)
  - **Input**
    - Graph G(V,E) mit V(G), sodass $\forall\ (v_1, v_2) \in E(G)\ mit\ v_1 \in V_1 \subset V\ und\ v_2 \in V_2 \subset V$
    - Menge von *Benutzern* U = V_1
    - Menge von *Ressourcen* R = V_2
  - **Output**
    - Minimale Anzahl von Rollen
  - **Vorarbeit**
    - Erstellung eines Graphen mit Kanten Benutzer-zu-Ressource aus der gegebenen RBAC-Instanz
    - Bestehende Rollen werden verworfen
  - Vorgehen durch Auflösen von Cliquen



DSN Research Group
Institute of Telematics, Faculty of Informatics

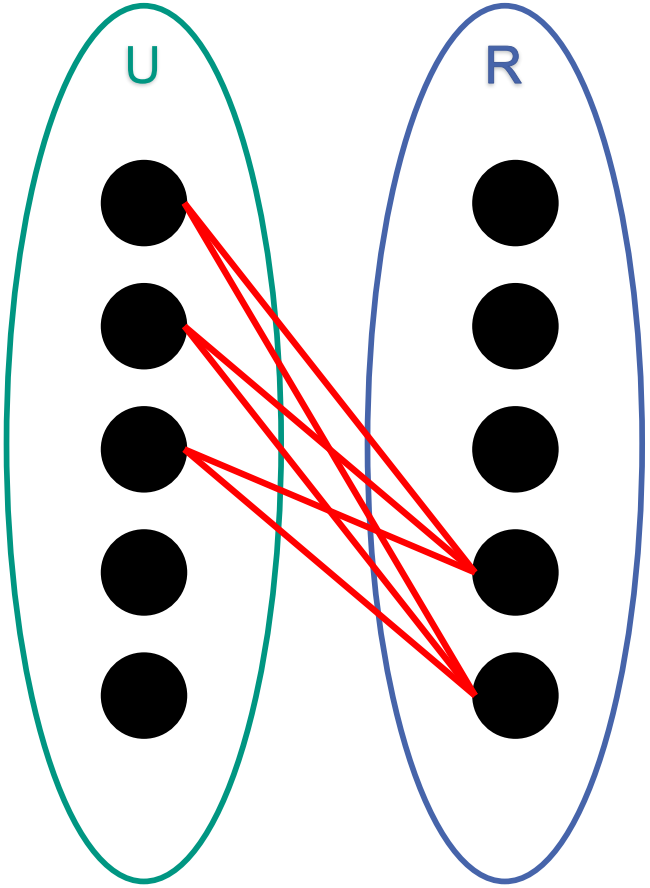
Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen



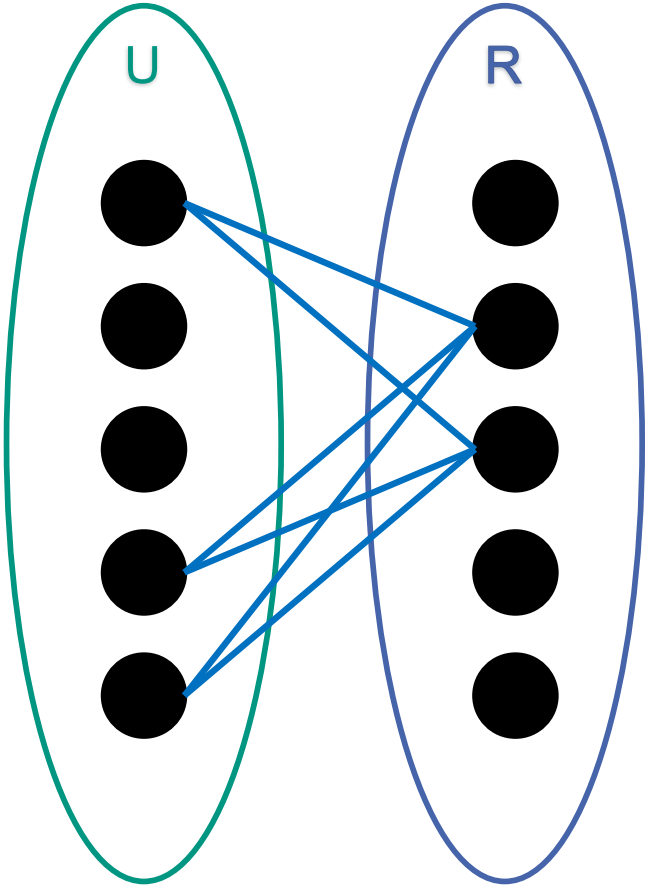
Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen:
  - Erste Biclique: *r1*



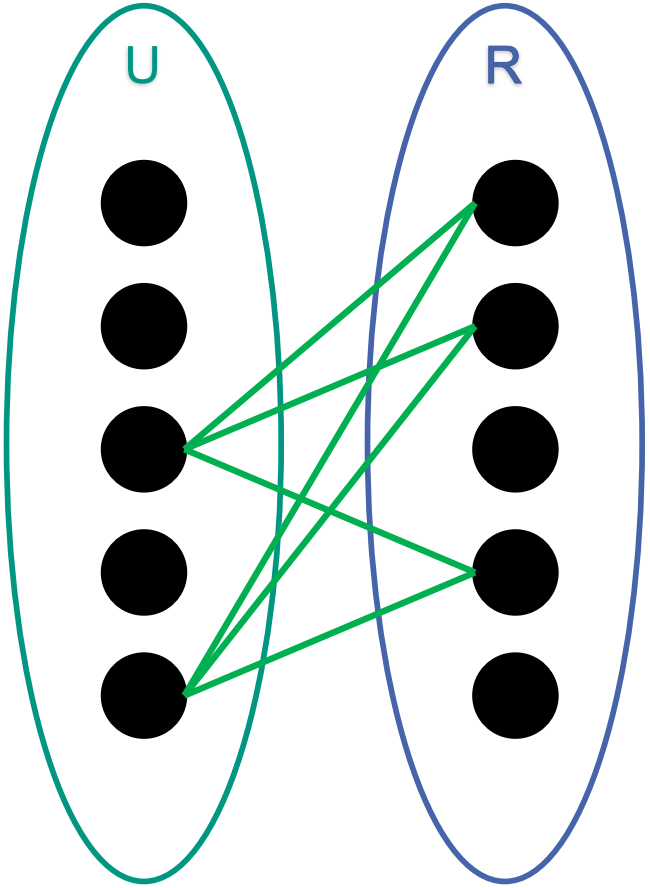
Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen:
  - Erste Biclique: *r1*
  - Zweite Biclique: *r2*



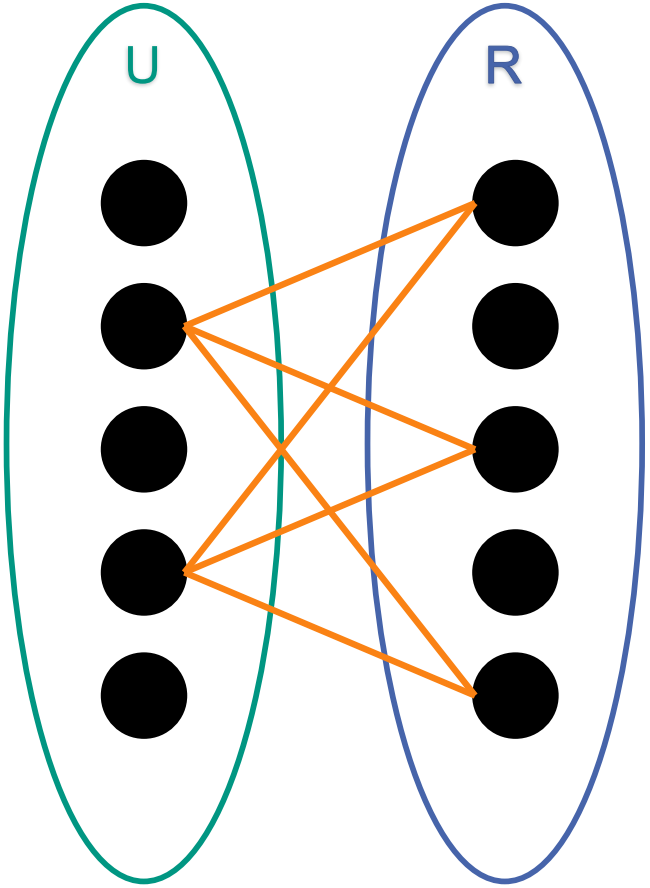
Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen:
  - Erste Biclique: *r1*
  - Zweite Biclique: *r2*
  - Dritte Biclique: *r3*



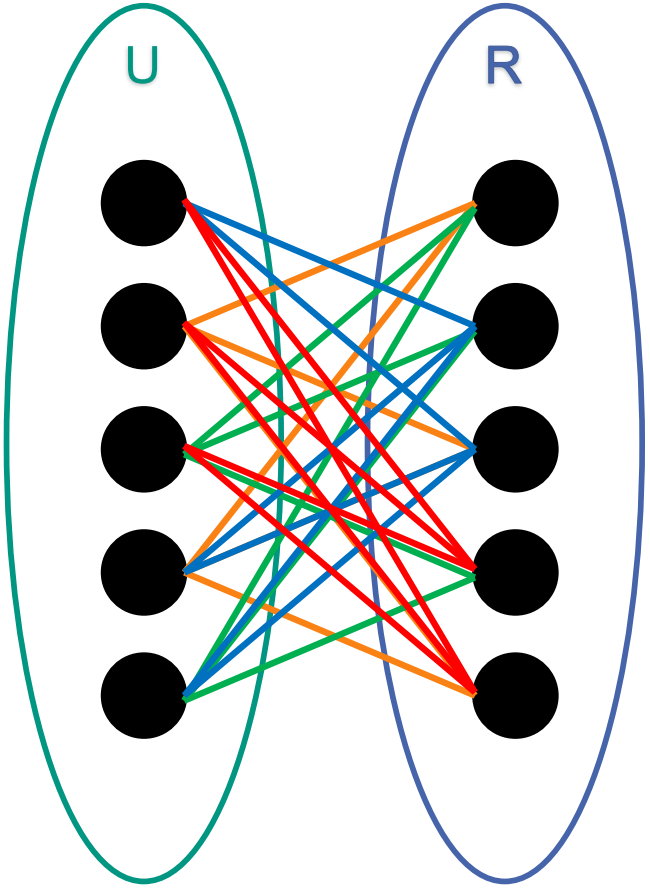
Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen:
  - Erste Biclique: *r1*
  - Zweite Biclique: *r2*
  - Dritte Biclique: *r3*
  - Vierte Biclique: *r4*



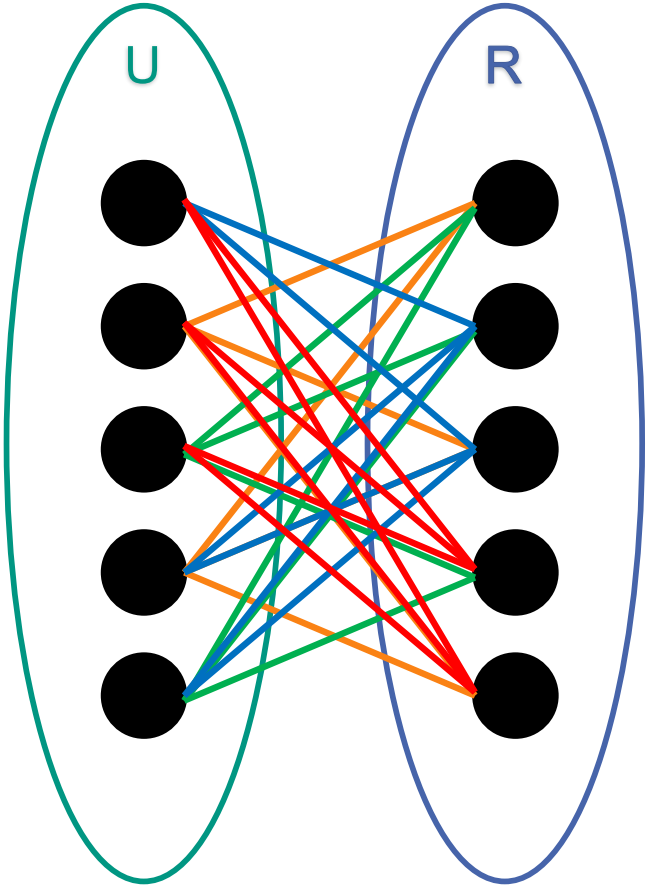
Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen:
  - Erste Biclique: *r1*
  - Zweite Biclique: *r2*
  - Dritte Biclique: *r3*
  - Vierte Biclique: *r4*
- Gefunden: 4 Bicliquen {*r1*, *r2*, *r3*, *r4*}



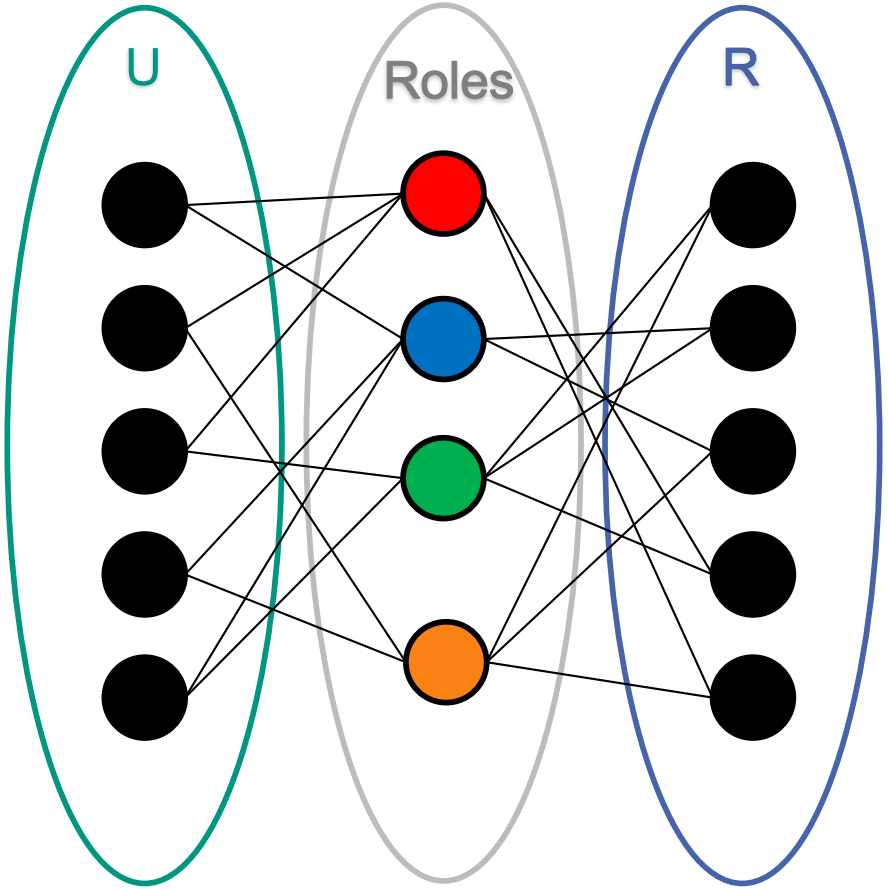
Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen:
  - Erste Biclique: *r1*
  - Zweite Biclique: *r2*
  - Dritte Biclique: *r3*
  - Vierte Biclique: *r4*
- Gefunden: 4 Bicliquen {*r1*, *r2*, *r3*, *r4*} ⇒ Entspricht der Anzahl an neuen Rollen



Ansatz basiert auf Role Minimization durch Minimum Biclique Cover (MBC) nach [EH+08]

- Ausgangspunkt: Benutzer-zu-Ressource-Beziehungen
  - Stellt bipartiten Graphen dar
  - Benutzer haben Rechte auf Ressourcen
- Schritt für Schritt Finden von Bicliquen, die Benutzer zu Gruppen zusammenfassen:
  - Erste Biclique: *r1*
  - Zweite Biclique: *r2*
  - Dritte Biclique: *r3*
  - Vierte Biclique: *r4*
- Gefunden: 4 Bicliquen {*r1*, *r2*, *r3*, *r4*} ⇒ Entspricht der Anzahl an neuen Rollen {*r1*, *r2*, *r3*, *r4*}



Algorithmus zum Lösen von MBC nach [EH+08]

- 1. Konstruiere einen Kanten-Dual-Graphen G' von G(V,E), sodass
  - G' = $(E, \{(e_1, e_2) | e_1 \; und \; e_2 \; eine \; Biclique \; von \; G \; bilden\})$
- 2. Finde eine Minimale Cliquen-Überdeckung (Minimum Clique Partition, MCP) von G' durch Graphenreduktion und –färbung
- 3. Jede Clique aus MCP(G') ist eine Menge von Kanten aus G
  - Die Knotenendpunkte der Kanten bilden Bicliquen
  - Somit wird das MBC-Problem gelöst
  - Eine Rolle je Biclique löst wiederum das Rollenminimierungsproblem

Ausblick und Zusammenfassung

- Es gibt weitere Ansätze zur Reduktion von RBAC-Instanzen, die in Kombination ein optimales Ergebnis liefern
  - Role Mining auf Basis von Matrizen-Algorithmen, Bottum-Up/Top-Down-Ansätze, Reduzierung von Rechtezuweisungen durch Kantenminimierung
- Problem
  - Geht Problem der Rollenbezeichnungen nicht an, Keine Hierarchien zwischen Rollen, existierende Rollen und Bedeutungen werden verworfen
- Vorteil
  - Test-Implementierung der Autoren führte in allen Testfällen zur Lösung des Minimalen-Rollen-Problems
- Implementierung
  - Die Umsetzung des Algorithmus nach [EH+08] fehlt noch
    - Schwierigkeiten beim Workaround über Cliquen-Berechnung
  - Eventuell gibt es fertige Bibliotheken, die ich in meiner Recherche-Arbeit übersehen habe

Literatur

- [EH+08] A. Ene, W. Horne, N. Milosavljevic: *Fast Exact and Heuristic Methods for Role Minimization Problems,* Hewlett-Packard, Princeton University, 2008
- [Wiki-BD] Wikipedia: *Bipartite dimension,* URL: https://en.wikipedia.org/wiki/Bipartite_dimension, 2017-07-25