Analyzing Security Policies

Sebastian Reitz

Ablauf

- Motivation und Ziele
- Matrixbasierte Systeme
- Rollenbasierte Systeme mit RBAC96
- FUB der Dresdner Bank
- Verwaltung von rollenbasierten Systemen
- Trust Management
- Fazit

MOTIVATION UND ZIELE

Motivation und Ziele

- Access Control
  - Zugriffsrechteverwaltung
  - Wer darf auf was zugreifen?
- Speichern von Berechtigungen
- Verwaltung von Berechtigungen
- Authentifizierung von Nutzern
- Theoretische Modelle für obige Ziele

MATRIXBASIERTE SYSTEME

Matrixbasierte Systeme

- Dienen zum Speichern von Zugriffsrechten
- Nutzer auf der einen Seite
- Dateien und Programme auf der anderen Seite
- Felder dienen zum Speichern von Rechten
- Mögliche Implementierung im HRU-Schema
  - Matrix aus Subjekten und Objekten
  - Kommandos bestehen aus Hinzufügen und Entfernen von Rechten, Objekten, Subjekten
  - System insgesamt sehr ineffizient
  - Problem der Leak Safety

ROLE BASED ACCESS CONTROL

Role Based Access Control

- Rollen als Zwischenschicht zwischen Nutzern und Rechten
- Rollen bestehen aus einer Menge von Berechtigungen
- Nutzer werden nun den Rollen zugewiesen
- Ermöglicht Gruppierung von Nutzern
  - Weniger Verwaltungsaufwand
  - Übersichtlichere Organisation

RBAC96

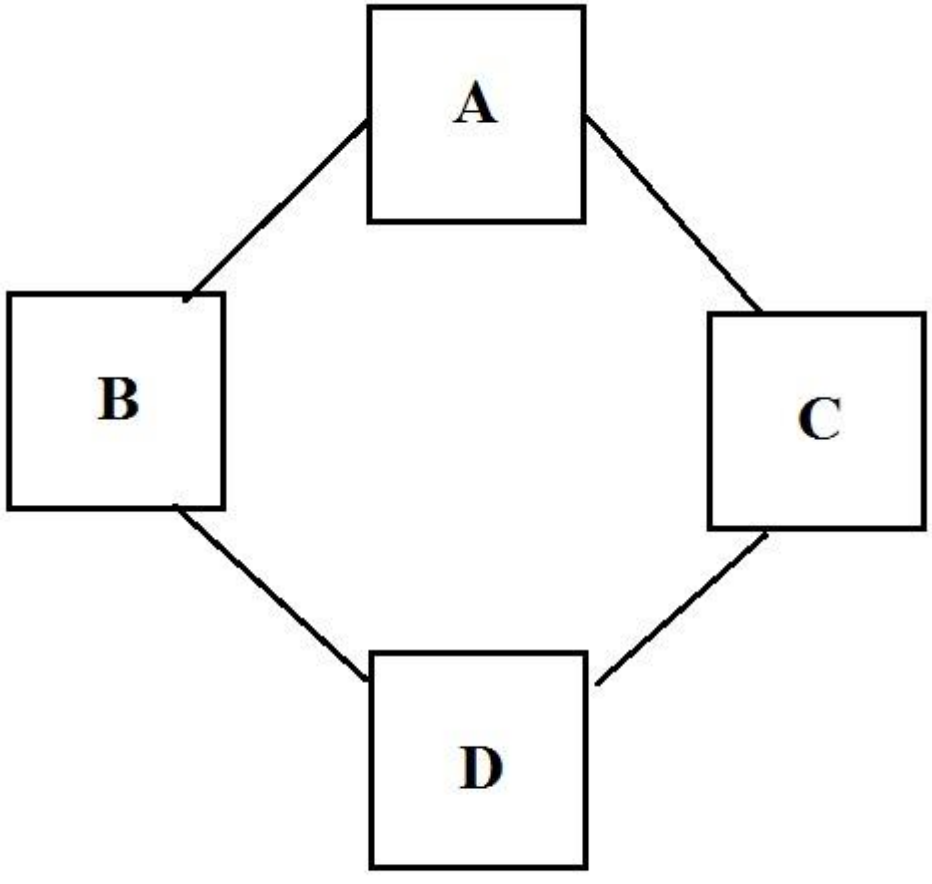
RBAC96

- Formales Model zur Organisation von Rechten
- Grundmengen für Nutzer, Rollen und Rechte(*U, R, P*)
- Zustand des Systems wird in 6 Relationen beschrieben
  - *UA* – Nutzer werden Rollen zugewiesen
  - *PA* – Rechte werden Rollen zugewiesen
  - *RH* – Die Hierarchie der Rollen
    - Azyklisch, transitiv, nicht reflexiv
  - CA – Wer darf Nutzer Rollen zuweisen
  - CR – Wer darf Nutzer von Rollen entfernen
  - CO – Welche Rollen schließen sich aus

RBAC96

- Es existieren Operationen zum Hinzufügen und Entfernen von Nutzern
- Hierarchische Organisationsstrukturen können auf die Rechteverwaltung übertragen werden

RBAC96 Beispiel

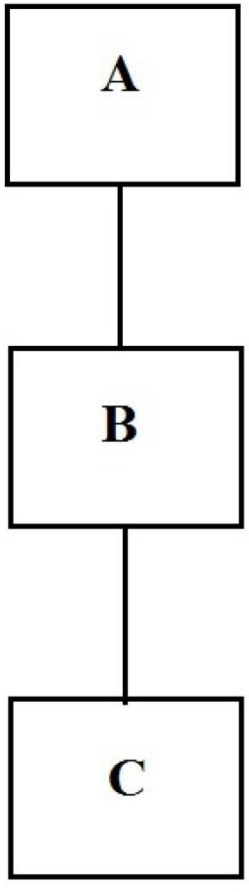


VERWALTUNG MIT ARBAC97

Verwaltung mit ARBAC97

- Modell, welches Verwaltung von RBAC 96 ermöglicht
- Geteilt in drei Bereiche
  - URA97
    - Verwaltung von Nutzern und Rollen
  - PRA97
    - Verwaltung von Rechten und Rollen
  - RRA97
    - Verwaltung der Rollenhierarchie

- Starkes Entfernen
- Schwaches Entfernen
- Vorbedingungen werden überprüft
- Admin-Rechte werden überprüft
- PRA analog



- Unterscheidung zwischen Rollentypen
  - Rollen aus Rechten und Rechtesammlungen
  - Rollen aus Nutzern und Nutzergruppen
  - Rollen welche alles enthalten können
- Rollen am Rand
  - Mögliche Probleme beim Zusammenführen von Relationen
- Rollen in der Hierarchie
  - Überprüfung schwierig
  - Komplexestes Problem von ARBAC97

DAS FUB DER DRESDNER BANK

Das FUB der Dresdner Bank

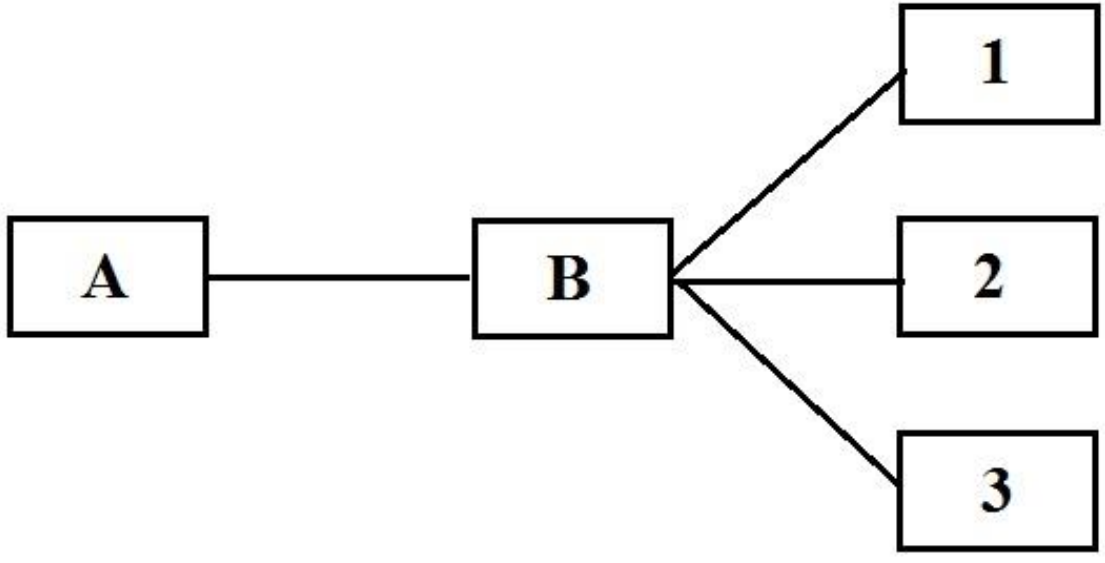
- Rollenbasiertes System in der Praxis
- 60 Anwendungen
- 42.000 Benutzerprofile
- 1300 Rollen
  - Kombination aus Funktion und Hierarchie
- Gute Trennung bei Verwaltung
- Abweichungen von RBAC
  - Rechte direkt Nutzern zuordnen
  - Keine Rollenhierarchie

TRUST MANAGEMENT DURCH ZERTIFIKATE

Trust Management durch Zertifikate

- Dient zur Autorisierung der Nutzer
- SPKI/SDSI
- Namensräume
- Delegation
- Zertifikate
- Zertifikatketten

Zertifikatkette



FAZIT

Fazit

- Matrixbasierte Systeme wenig relevant
  - Unpraktisch
  - Langsam
- Rollenbasierte Systeme relevanter
  - Gute Rechteverwaltung
  - Übersichtliche Organisation
- SPKI/SDSI als gute Ergänzung für Trust Managements