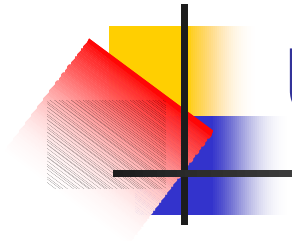
Authentifizierung

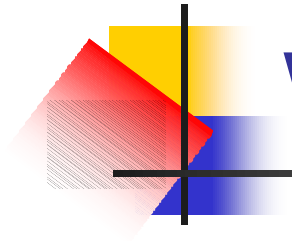
Benutzerverwaltung mit Kerberos

Referent: Jochen Merhof



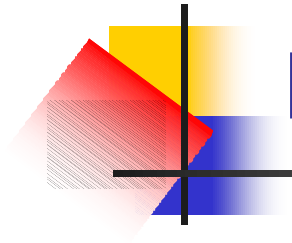
Überblick über Kerberos

- Entwickelt seit Mitte der 80er Jahre am MIT
- Netzwerk-Authentifikations-Protokoll
  (Needham-Schroeder)
- Open-Source Entwicklung und kommerzieller Vertrieb



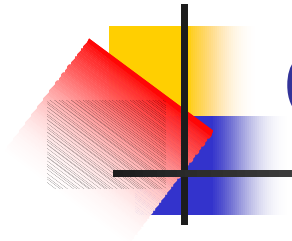
Warum wurde Kerberos entwickelt?

- Immer größere Netze
- Schutz von Ressourcen vor nicht authorisiertem Zugriff
- Nicht vertrauenswürdige Netze z.b. auch durch Verwendung von wireless-Komponenten



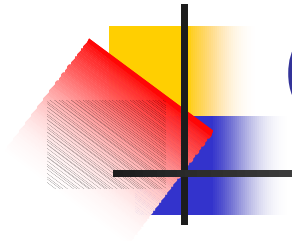
Kerberos

- Authentifizierungsdienst
- Netz gilt als unsicher
- Client muss seine Identität beweisen



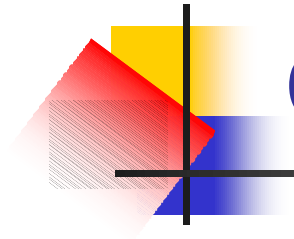
Grundbegriffe

- Prinzipal: Ist der Benutzer, Client oder die Applikation, welche an der Kommunikation teilnimmt.
- Private Key: Ist der geheime Schlüssel, der nur dem Prinzipal und dem Authentication Server bekannt ist.
- Session Key: Ist ein Schlüssel, der vom TGS für eine bestimmte Kommunikation vergeben wird.



Grundbegriffe(2)

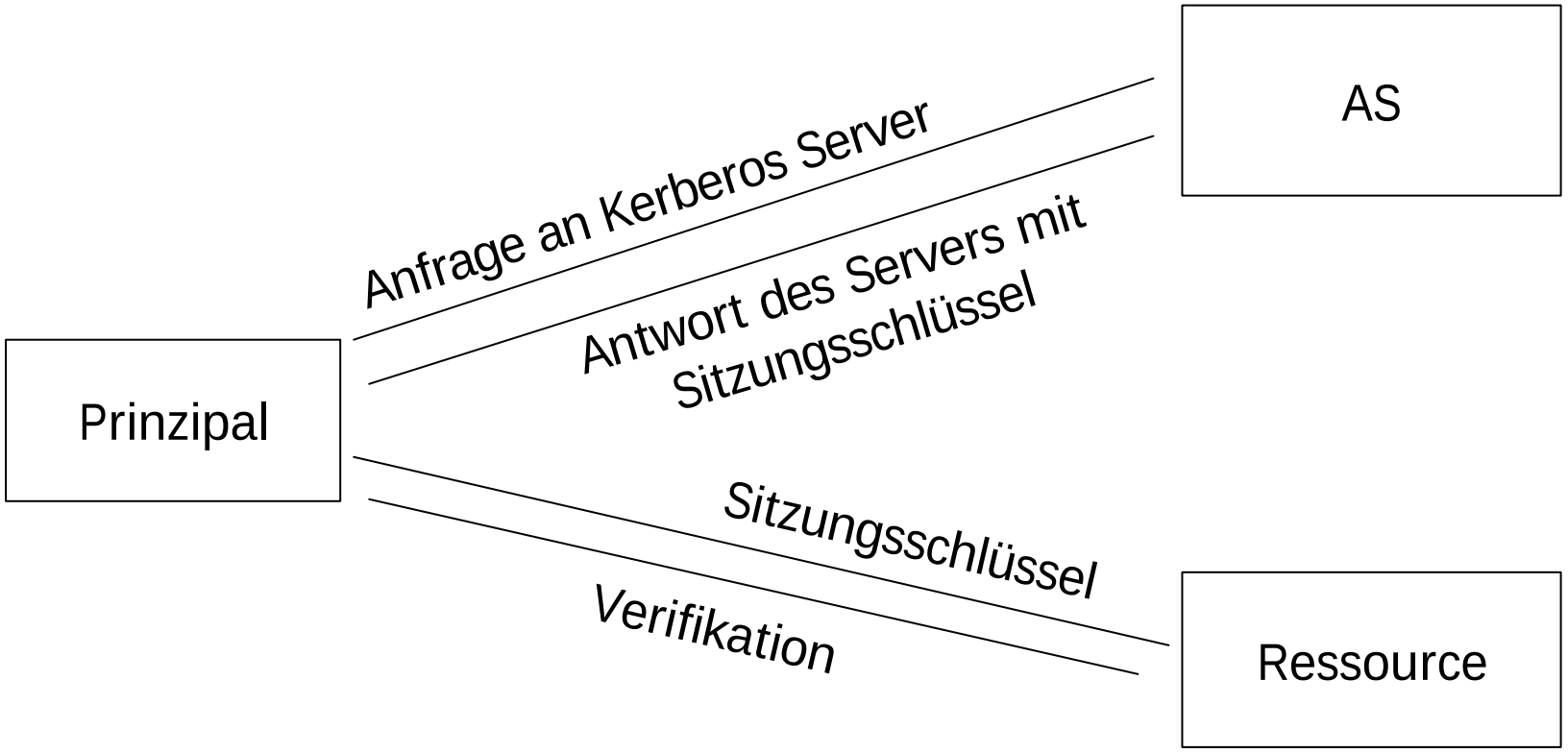
- AS: Authentication Server; authentifiziert die sich bei ihm bewerbenden Benutzer und Ressourcen
- TGS: Ticket-Granting-Server; vergibt Tickets für die Kommunikation zwischen Prinzipal und Ressourcen
- KDC: Key-Distribution-Center; setzt sich aus AS und TGS zusammen

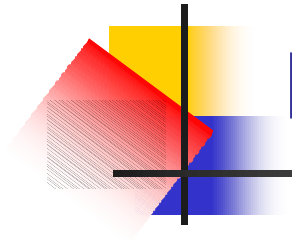


Grundlegende Merkmale von Kerberos

- User muss sich beim ersten Login authentifizieren
- Aus dem Passwort wird ein Key generiert, der zum entschlüsseln der Nachricht des AS dient.
- Verschlüsselung mit z.b. DES (symmetrisch); Kerberos 5 bietet noch andere Verschlüsselungsverfahren
- Jeder Prinzipal und jeder Dienst hat einen eigenen Private Key
- Der Authentication Server kennt alleine alle Private Keys von sämtlichen Usern und Diensten

Kommunikationsschritte

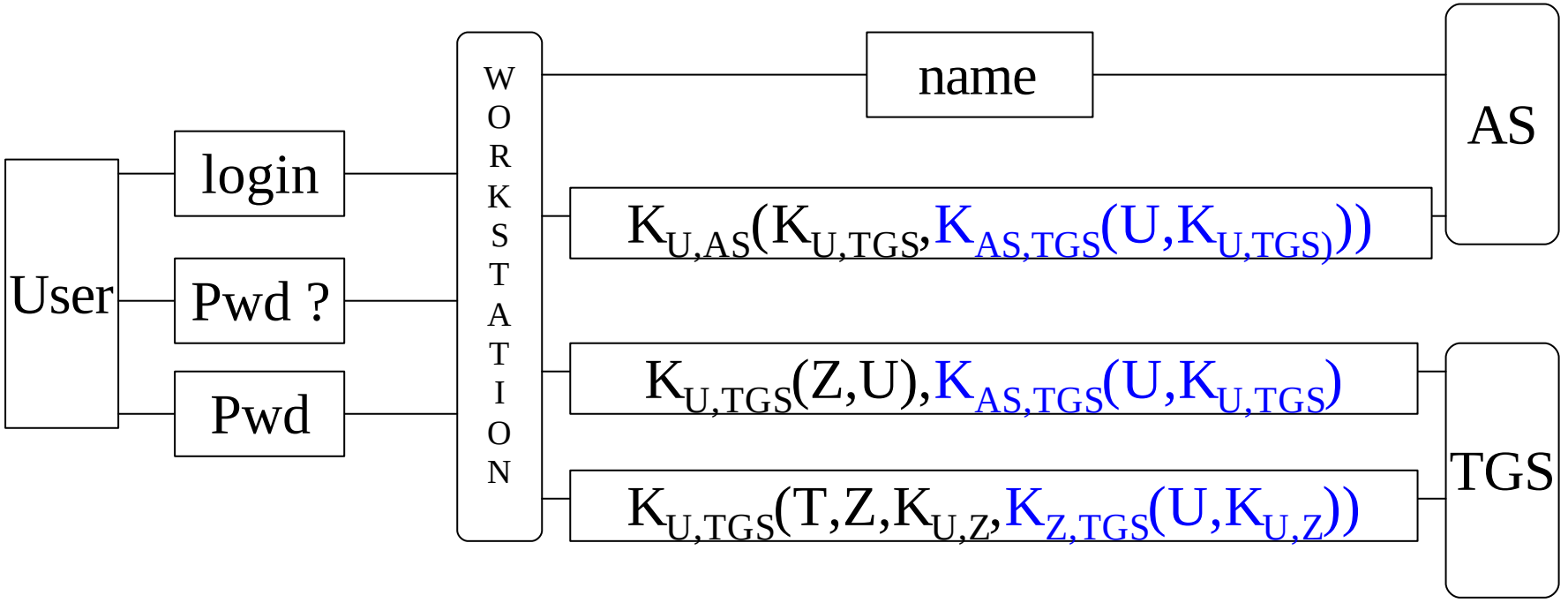




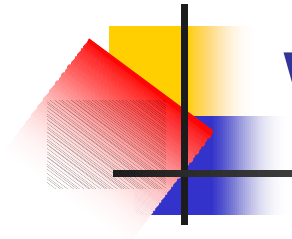
Kommunikationsschritte

- Hier jeweils neue Authentifizierung nötig
- Wiederholte Übertragung von Packeten, die mit dem Private Key vom Prinzipal verschlüsselt sind
- Passwort auf HDD zu sichern zu gefährlich (Beglaubigungscache)
- Umgehung dieser Probleme mit dem TGS

Kommunikation im Detail

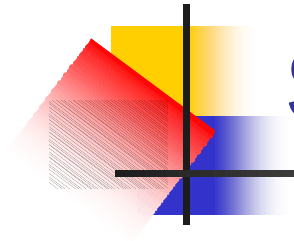


(Z steht für Zielressource)
(T steht für Time-Stamp)



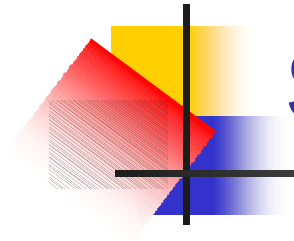
Weitere Software-Komponenten

- Encryption library basiert auf dem Data Encryption Standard. Sie bietet unterschiedliche Methoden der Verschlüsselung (unterschiedlich für hohe Sicherheit oder große Geschwindigkeit)
- Database administration programs bieten alle benötigten Tools zur Administration der Datenbank.



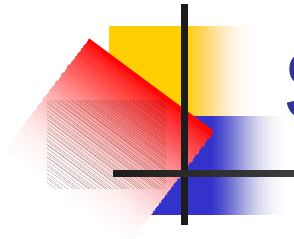
Software-Komponenten(2)

- Administration server ist das Lese- und Schreibinterface zu der Datenbank. Er läuft nur auf dem Rechner, auf dem auch die Kerberos Datenbank läuft, wohingegen die Clients des Servers auf jeden beliebigen Rechner laufen kann.
- Applications sind z. B. Programme für das Einloggen in Kerberos, für das Ändern von Paßworten oder das Anzeigen oder Zerstören von Tickets.



Software-Komponenten(3)

- Database propagation software hat die Aufgabe, der Verteilung von Kopien der Kerberos Datenbank. Es ist möglich, Kopien der Datenbank und des authentication servers auf vielen verschiedenen Rechnern laufen zu haben (Ausfallsicherheit bei nur einem Rechner mit der Datenbank Kontra Sicherheit bei der Verbreitung von Kopien der Datenbank). Jede sogenannte Slave-Machine erhält in regelmäßigen Abständen Updates von der Master Datenbank.



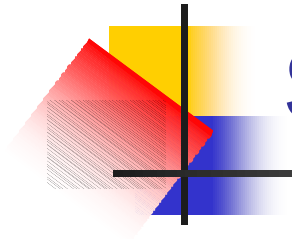
Schwachstellen von Kerberos

Mögliche Angiffspunkte

- TGT fällt in falsche Hände => Netzwerkressource kann von Eindringling genutzt
- Hack-Angriff auf Tickets zwischen Prinzipal und KDC
- Kompromittierter Kerberos-Server

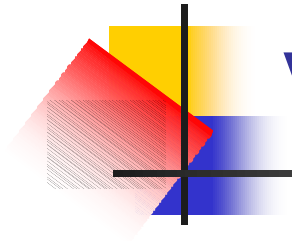
Konsequenzen

- TGT hat begrenzte Gültigkeit
- Diese Tickets haben nur eine Gültigkeit von 5 Minuten
- Server physikalisch absichern



Schwachstellen von Kerberos(2)

- Bei Kerberos 4: Feste Verschlüsselung (DES)
  =>Gleicher Aufbau der Tickets; Time-Stamp enthalten (siehe Paper 4.2)
  =>Entschlüsseln möglich, da das Format eines Teiles der Nachricht bekannt ist
- Wichtiger Punkt: Time-Stamps
  Synchronisierte Urzeiten im gesamten Netz nötig
  => Replay-Angriffe



Vorteile von Kerberos

- Benutzerpasswort wird nur einmal übertragen
- Sämtliche Tickets werden verschlüsselt
- Gültigkeit der Tickets beschränkt
- Ressourcenverwaltung zentral möglich
- Verwendete Sicherheitsmechanismen zentral beeinflussbar

Anwendung in aktuellen Systemen

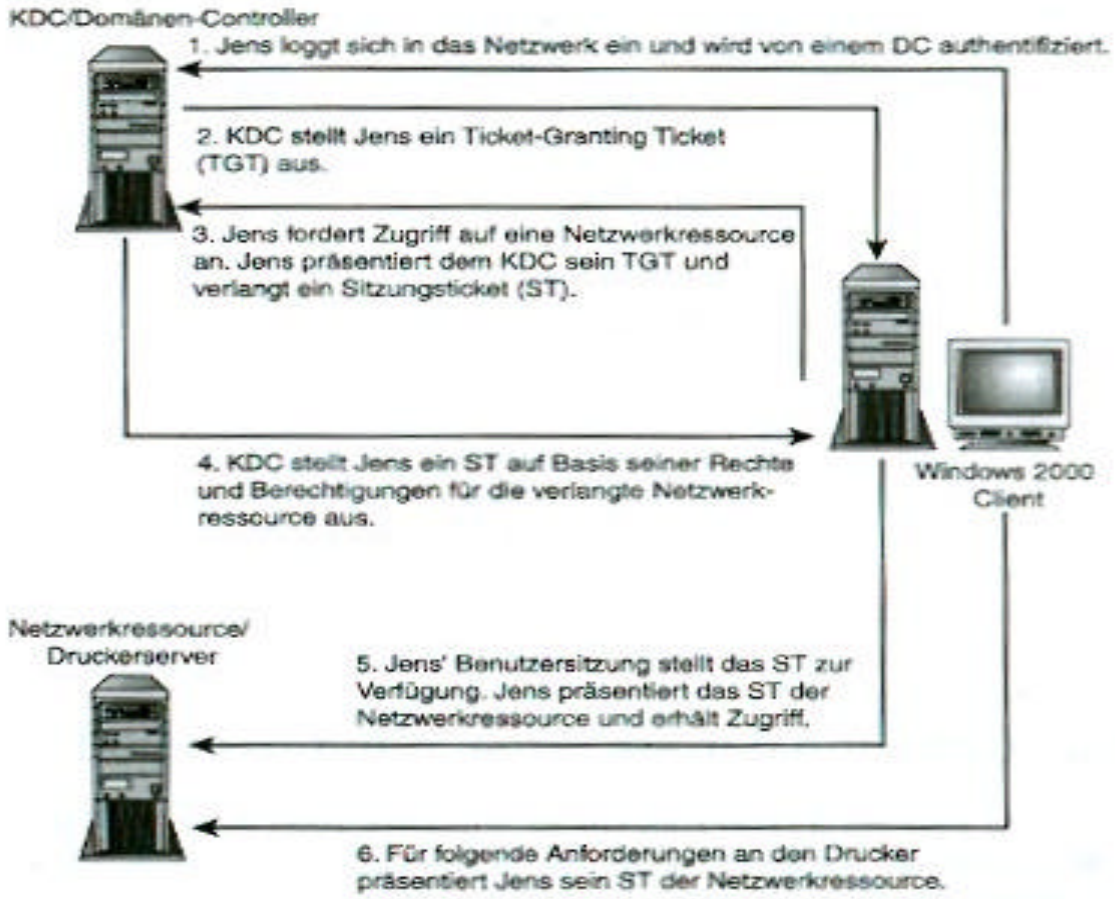


Abb. 11.2: Anmeldung und Zugriff auf eine Netzwerkressource unter Windows 2000

Anwendung in aktuellen Systemen(2)

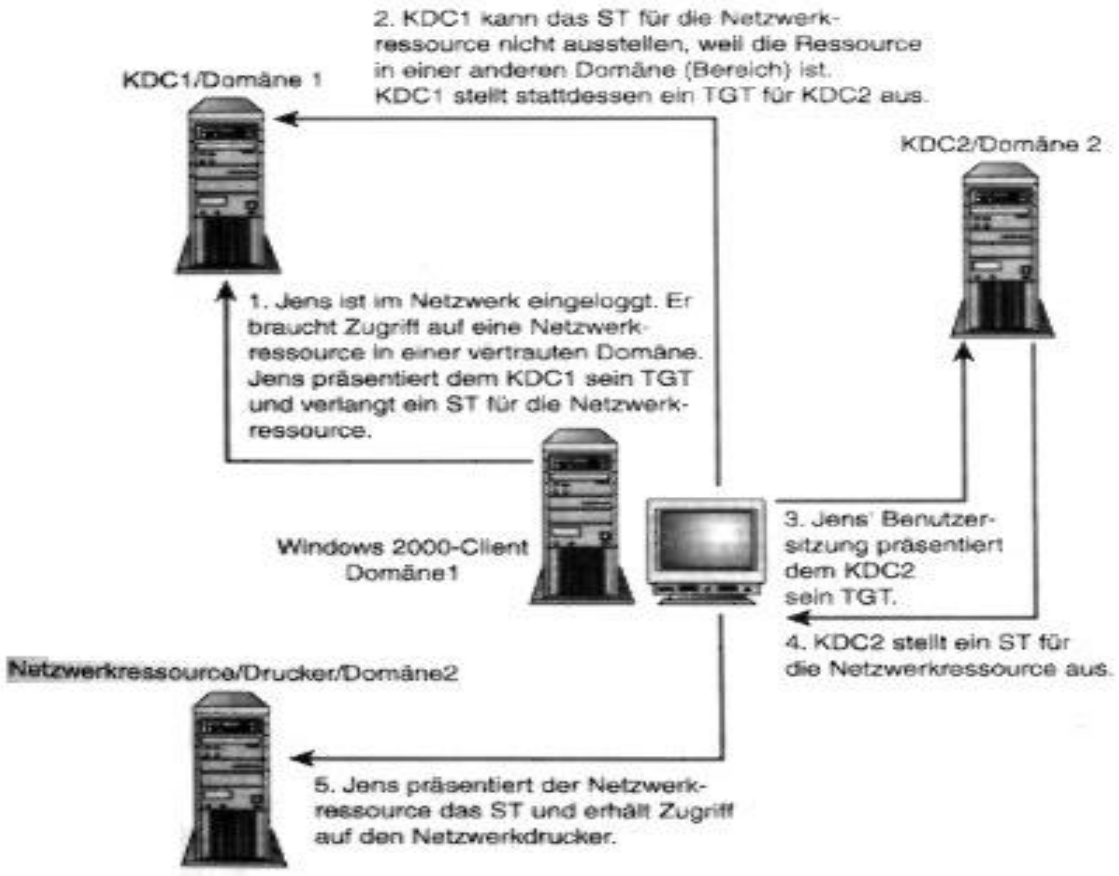


Abb. 11.3: Zugriff über Kerberos auf Ressourcen in einer anderen Domäne

Anwendung in aktuellen Systemen(3)

Transitive Vertrauensstellung

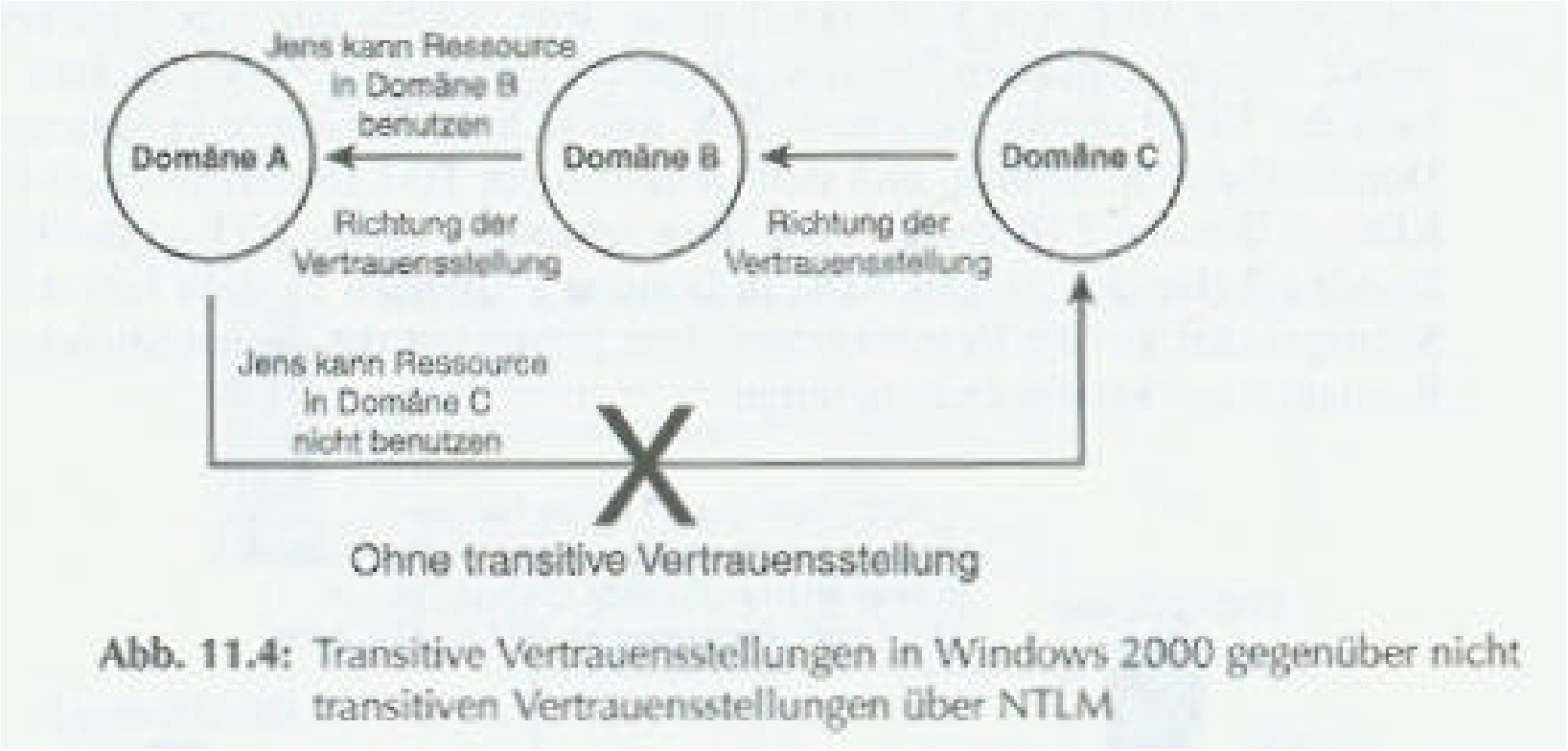
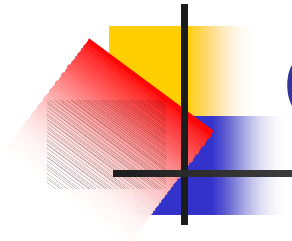


Abb. 11.4: Transitive Vertrauensstellungen in Windows 2000 gegenüber nicht transitiven Vertrauensstellungen über NTLM



Quellen

- [1] Secure Computing: THREADS AND SAFEGUARDS; Rita C. Summers McGraw-Hill, 1997
- [2] Windows 2000 Security: Kryptographie, Kerberos, Authentifizierung; Jeff Schmidt, Markt+Technik, 2001
- [3] Hackerabwehr und Datenschutz: Angriff, Diagnose, Abwehr; Aviel Rubin Addison-Wesley, 2002
- [4] Kerberos Autentifikation; Bindrich http://wwwbs.informatik.htw-dresden.de/svortrag/ai95/Bindrich/kerberos.html
- [5] Red Hat Linux 7.3: Das Offizielle Red Hat Linux Referenzhandbuch http://www.europe.redhat.com/documentation/rhl7.3/rhl-rg-de-7.3/ch- kerberos.php3
- [6] Red Hat Linux 7.3: Das Offizielle Red Hat Linux Referenzhandbuch http://www.europe.redhat.com/documentation/rhl7.3/rhl-rg-de-7.3/s1-kerberos- whynot.php3
- [7] Red Hat Linux 7.3: Das Offizielle Red Hat Linux Referenzhandbuch: Kerberos-Terminologie http://www.europe.redhat.com/documentation/rhl7.3/rhl-rg-de-7.3/s1-kerberos-terminology.php3
- [8] Kerberos: The Network Authentication Protocol http://web.mit.edu/kerberos/www/papers.html