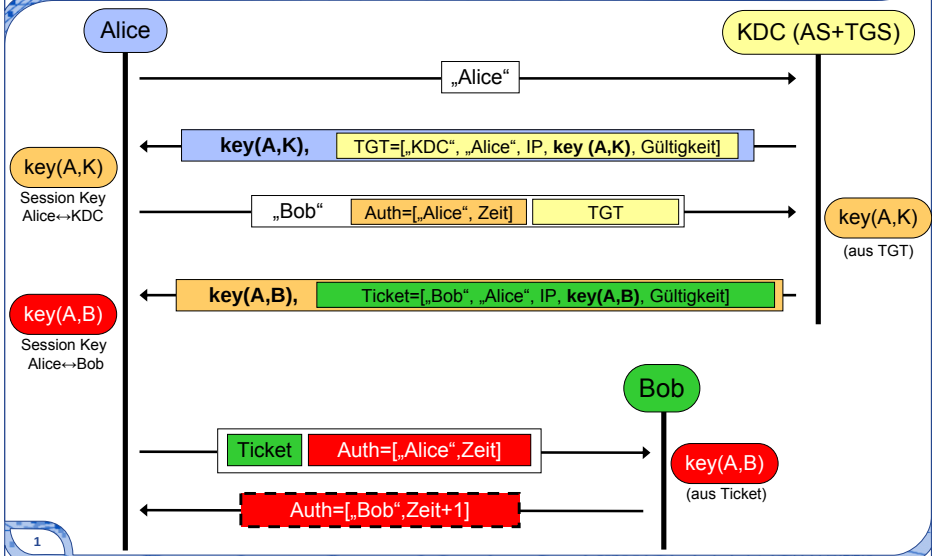
Netzsicherheit
Architekturen und Protokolle
Kerberos

1. Einführung
2. Kerberos Version 4
3. Kerberos Version 5

Wdh: Kerberos v4 (vereinfacht)



Kerberos Version 5

- Gleiches Konzept wie bei Kerberos v4, aber
  - Änderungen
    - verbesserter Schutz der Benutzer-Passwörter
    - Nachrichtenformat
      - v4: festes Format
      - v5: ASN.1 (Abstract Syntax Notation One)
    - freie Wahl des Verschlüsselungsverfahren
  - Erweiterungen
    - **Weitergabe der eigenen Rechte**
    - **flexiblere Gültigkeiten von Tickets**
  - Optimierungen
    - keine doppelte Verschlüsselung des TGT

Rechteübertragung

- Problem in Kerberos v4
  - Absender IP-Adresse im Ticket enthalten
  - Änderung der Ticket IP-Adresse nicht möglich

  → Übertragung der Rechte nicht möglich

→ welche Anforderungen würden Sie an ein übertragbares Ticket stellen?

→ welche Tickets würden Sie in Kerberos übertragbar machen?

→ wen würden Sie über die Übertragbarkeit von Tickets entscheiden lassen?

Rechteübertragung

- Anforderungen an übertragbares Ticket
  - zeitliche Beschränkung der Rechteübertragung
  - Beschränkung der übertragenen Rechte durch Besitzer
- Mögliche übertragbare Tickets
  - *Ticket Granting Ticket*
  - *Tickets*
- Wer darf über Übertragbarkeit entscheiden?
  - Nutzer (beim Beantragen)
  - KDC (über Richtlinie beim Ausstellen)
  - Ressource (über Akzeptanz bei der Annahme → Transparenz nötig)

Übertragbare Tickets in Kerberos v5

- Übertragbare Tickets
  - Forwardable TGT: übertragbares Ticket-Granting Ticket
  - Proxy Ticket: übertragbares Ticket
- Gültigkeit von Tickets
  - Angabe der IP-Adresse(n), von wo Ticket verwendet werden kann
  - überall gültig wenn keine IP, mehrere Adressen möglich
  - Restriktion durch IP-Spoofing umgehbar
    - *"Including the network addresses only makes it more difficult, not impossible, for an attacker to walk off with stolen credentials and then use them from a "safe" location."* (RFC1510)
- weiteres
  - Erkennung übertragbarer Tickets durch Flag
  - Übergabe des dazugehörigen Sitzungs-Schlüssel mit dem übertragbaren Ticket

Einschränkungen übertragbarer Tickets

- Sicherheitsrichtlinien des KDC regelt Vergabe von übertragbaren Tickets
  - z.B. Einschränkung der Ausgabe von Tickets ohne IP-Adresse
- Jede Ressource (Anwendung) regelt die Akzeptanz von übertragbaren Tickets selbst
  - erkennt übertragenes Ticket durch Flag „Proxy" bzw. „Forwarded"
  - Sicherheitsrichtlinien für jede Ressource (Anwendung)
  - Akzeptanz bzw. Ablehnung von Tickets ohne IP-Adresse

Lebenszeit von Tickets

- Problem der Lebenszeit von Tickets
  - feste und begrenzte Lebenszeit in Kerberos v4
  - in Kerberos v5 Beschreibung wg. ASN.1 kein Problem
  - Gefahr durch langlebige Tickets
    - Widerrufen schwierig
    - keine Auswirkung von geänderten Zugriffsrechten auf bereits ausgestellte Tickets
- Zwei neue Arten von Tickets in Kerberos v5
  - *erneuerbare Tickets* (langfristig gültige Tickets)
  - *zukünftige Tickets* (Gültigkeitsbeginn in der Zukunft)

  → *auf folgenden Folien*

Erneuerbare Tickets

- Einsatzgebiet *erneuerbarer Tickets*
  → regelmäßige Wartungsarbeiten wie Batch-Jobs
  - Renewable-Flag im Ticket gesetzt
  - Gültigkeit des Tickets bis: End-Time
    - festgelegt in KDC-Konfiguration
    - Überprüfung durch Ressource
  - Einschränkung: Regelmäßige Erneuerung des Tickets möglich (jeweils vor End-Time)
    - Erneuerung des Tickets durch KDC maximal bis Renew-Till
    - Überschreitung der End-Time: Ticket nicht mehr erneuerbar
  - Widerrufen der Tickets nach Ausstellung jederzeit möglich
    - müssen nur minimale Zeit gespeichert werden (wegen Behandlung von abgelaufenen Tickets)
  - Speicherung abgelaufener Tickets im KDC *nicht* notwendig

Zukünftige Tickets

- Einsatzgebiete *zukünftiger Tickets*
  → beispielsweise Backup
  - Flags
    - May-postdate-Flag im TGT
      - Flag gesetzt: Ausstellung zukünftiger Tickets möglich
    - Invalid-Flag und Postdated-Flag im Ticket gesetzt
    - Start-Time in der Zukunft
  - Wiedervorlage des Ticket zum Startzeitpunkt beim KDC
    - löschen des Invalid-Flags
    - Widerruf des Tickets nach Ausstellung möglich
  - Jede Anwendung regelt Akzeptanz von zukünftigen Tickets selbst
    - Postdated-Flag bleibt nach „Aktivierung“ bestehen

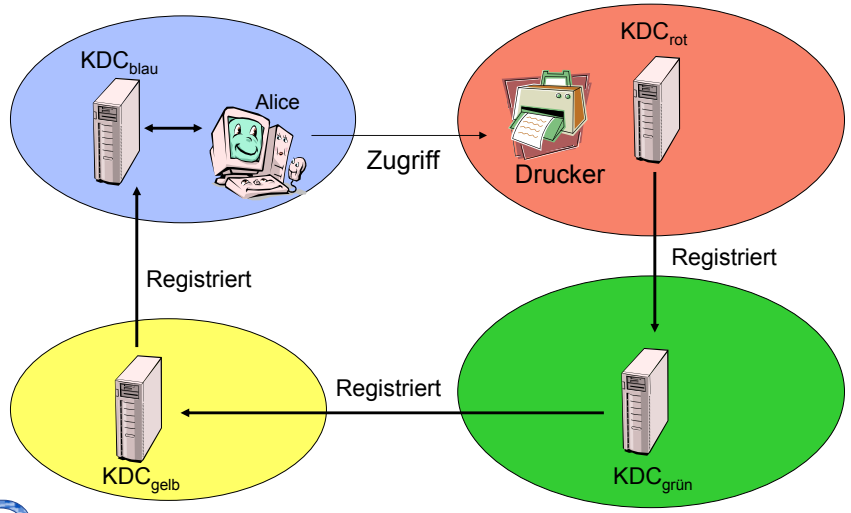
Vorteile/Nachteile Rechteübertragung

- Vorteile
  - Protokollierung aller Rechteübertragungen durch KDC
  - Beschränkung der Rechteübertragungen durch KDC und Anwendung
- Nachteile
  - Verringerung der Performanz durch Kontaktierung des KDC
  - Komplizierte Zugriffsbeschränkungsregeln im KDC und in den Anwendungen

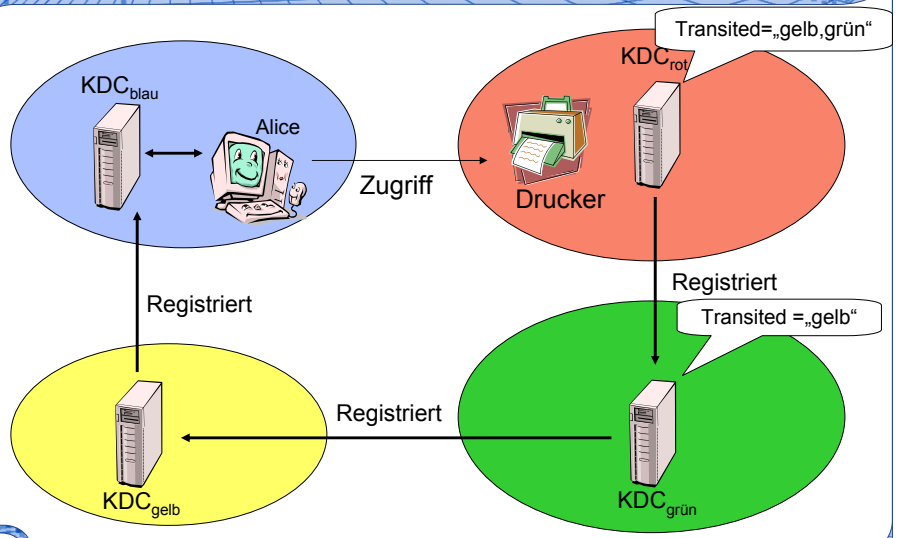
Inter-Domänen Authentifizierung

- Inter-Domänen Authentifizierung
  - v4: nur *direkte Authentifizierung*
  - v5: *Verkettung* von Inter-Domänen Tickets möglich
  - Transited Feld im Ticket
    - Auflistung aller zur Authentifizierung zu durchlaufener Domänen
  - Regelung des Umgangs mit verketteten Inter-Domänen Tickets durch Sicherheitsrichtlinien in Applikation
    - Standard: kürzester Weg durch die Hierarchie bildet Menge vertrauenswürdiger Domänen
- Hierarchische Domänen
  - KDC registriert sich als Client bei KDC der Vaterdomäne
  - Anlehnung an Internet- oder X.500 Name

Inter-Domänen-Authentifizierung



Inter-Domänen-Authentifizierung



Angriffe

Welche Angriffe sind auf diese Inter-Domänen-Authentifizierung möglich?

Password-Guessing Angriffe verhindern

- Preauthentication-Data
  - in **`AS_REQ`** enthalten
  - Zeitstempel mit Master-Secret des Clients verschlüsselt
  - Authentication Server antwortet nur mit **`AS_REP`**, falls Zeitstempel korrekt entschlüsselt wird

Diskussion: Password-Guessing Angriffe verhindern?

Welche Angriffe werden mit Preauthentication-Data verhindert?

Welche Angriffe sind weiterhin möglich?

Password-Guessing Angriffe verhindern

- Weiterhin möglicher Angriff
  - Ticket für Zugriff auf einen Benutzer beantragen
  - Offline Password-Guessing Angriff auf dieses Ticket
- Markieren von Benutzereinträgen
  - TGTs nur für menschliche Nutzer
  - KDC stellt keine Tickets zu Clients aus, deren Master-Key aus einem Passwort abgeleitet wird (=meist Benutzer)
- verbleibende Risiken
  - Brute-Force-Angriffe: Passwort raten, daraus Preauthentication-Data
    - dauert lange und Logging von fehlgeschlagenen Authentifizierungsversuchen am KDC

Zusammenfassung Kerberos v5

Neuerungen gegenüber Kerberos v4

- flexibles Nachrichtenformat durch ASN.1
- längere Ticketlebenszeit
  - erneuerbare Tickets
  - zukünftige Tickets
- Übertragung von Rechten möglich
  - Forwardable TGT
  - Proxy Ticket
- mehrstufiges Domänenkonzept

Bewertung Kerberos

- Vorteile
  - nur ein Passwort zur Anmeldung am Netz (*Single-Sign-On*)
  - sichere netzwerkweite Authentifizierung und Autorisation
  - Dienst und Nutzer authentifizieren sich gegenseitig
  - Unterstützung von Vertraulichkeit und Integrität
  - basiert fast ausschließlich auf symmetrischen Verfahren
- Nachteile
  - KDC Master Key befindet sich auf dem KDC
    - Kompromittierung legt alle Client Master Keys offen
  - alle Ressourcen müssen angepasst werden (Kerberized)
  - Authentifizierung basiert auf IP-Adressen
    - IP-Spoofing einfach
  - Passwort-Überprüfung durch Challenge-Response nur optional
  - enge Synchronisation der Uhren der Netzkomponenten notwendig

Fragen zu Kerberos

1. Trennen Sie Funktionalitäten des KDCs in Authentication Server und Ticket Granting Server. Welche Unterschiede bzw. Gemeinsamkeiten bestehen zwischen den beiden?
2. Beschreiben Sie kurz den Zugriff auf eine Ressource, deren Systemuhr um mehr als 5 Min. nachgeht.
3. Wie könnte ein Angreifer sich als Alice ausgeben, wenn die Übertragung vom Master-Copy auf einen Slave nicht durch einen kryptographischen Hash geschützt wäre?
4. Geben Sie alle Nachrichten in ihrer zeitlichen Reihenfolge an, die versandt werden, angefangen bei einloggen bis zum Zugriff auf eine Ressource in einer fremden Domäne. Geben Sie zu jeder Nachricht an, mit welchem Schlüssel diese verschlüsselt ist.
5. Warum lässt man nicht die Ressource die Gültigkeit von erneuerbaren und zukünftigen Tickets überprüfen?

Literatur

Sichere Netzwerkkommunikation, Bless, Blaß, Conrad, Hof, Kutzner, Mink, Schöller, Springer.

- Kaufmann, Perlman, Speciner: „Network Security – Private Communication in a Public World“, Prentice Hall PTR, 2002, ISBN 0130460192
- RFC 1510 J. Kohl, C. Neuman: „The Kerberos Network Authentication Service (V5)“, September 1993, http://tools.ietf.org/rfc/rfc1510.txt
- RFC 4120 C. Neumann, T.Yu, S. Hartman, K. Raeburn: „The Kerberos Network Authentication Service (V5)“, July 2005, http://tools.ietf.org/rfc/rfc4120.txt
- Needham, R.M., and Schroeder, M.D.: „Using Encryption for Authentication in Large Networks of Computers“, Communications of the ACM, Vol. 21, Number 12, Pages 993-999, Dezember 1978
- RFC 2623 M. Eisler: “NFS Version 2 and Version 3 Security Issues and the NFS Protocol's Use of RPCSEC_GSS and Kerberos V5”, June 1999, http://tools.ietf.org/rfc/rfc2623.txt
- RFC 2712 A. Medvinsky, M. Hur: “Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)”, October 1999, http://tools.ietf.org/rfc/rfc2712.txt
- RFC 2942 T. Ts'o: “Telnet Authentication: Kerberos Version 5”, September 2000, http://tools.ietf.org/rfc/rfc2942.txt
- RFC 3244 M. Swift, J. Trostle, J. Brezak: “Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols”, February 2002, http://tools.ietf.org/rfc/rfc3244.txt