Sicherheitsmechanismen des Betriebssystems

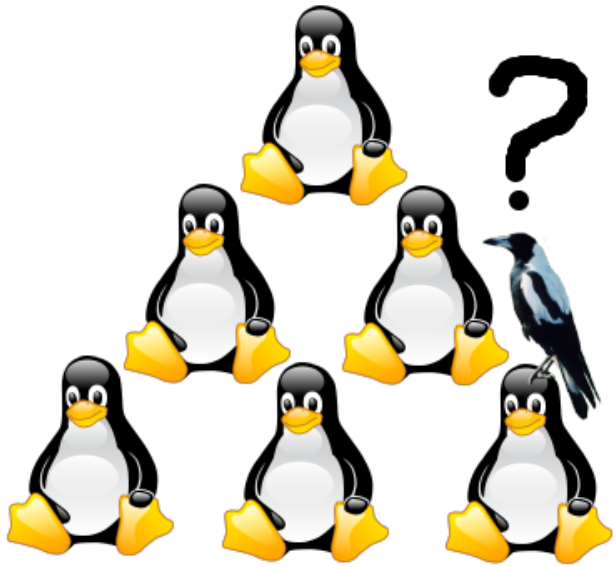
Andre Ufer, Oliver Burger

DHBW Stuttgart - Campus Horb

24. November 2011

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Linux



DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Linux

- ...entstand Anfang der 90er Jahre

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Linux

- ...entstand Anfang der 90er Jahre
- ...heute vor allem im Server- und Embedded-Bereich weit verbreitet

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Benutzer, Gruppen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Benutzer, Gruppen

- strikte Trennung Benutzer - Administrator (*root*)

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Benutzer, Gruppen

- strikte Trennung Benutzer - Administrator (*root*)
- (fast) alle Systemdienste starten als eigenständiger Benutzer, nicht als *root*

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Benutzer, Gruppen

- strikte Trennung Benutzer - Administrator (*root*)
- (fast) alle Systemdienste starten als eigenständiger Benutzer, nicht als *root*
- (lokale) Verwaltung über drei Dateien

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Benutzer, Gruppen

- strikte Trennung Benutzer - Administrator (*root*)
- (fast) alle Systemdienste starten als eigenständiger Benutzer, nicht als *root*
- (lokale) Verwaltung über drei Dateien
- *passwd*, *shadow*, *group*

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/passwd

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/passwd

- Sieben Spalten getrennt durch „:“

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/passwd

- Sieben Spalten getrennt durch „:“
- Benutzername, Passwort, Benutzer-ID, Primärgruppen-ID, langer Name, HOME-Verzeichnis, Login-Shell

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/passwd

- Sieben Spalten getrennt durch „:“
- Benutzername, Passwort, Benutzer-ID, Primärgruppen-ID, langer Name, HOME-Verzeichnis, Login-Shell

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
...
polkituser:x:489:488:system user for policykit:/:/sbin/nologin
...
oli:x:10001:10001:Oliver Burger:/home/oli:/bin/bash
postgres:x:485:478:system user for postgresql9.0:/var/lib/pgsql:/bin/bash
apache:x:484:476:system user for php:/var/www:/bin/sh
ftp:x:483:475:system user for proftpd:/var/ftp:/bin/false
...
```

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/group

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/group

- Vier Spalten getrennt durch „:“

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/group

- Vier Spalten getrennt durch „:“
- Gruppenname, Passwort, Gruppen-ID, Gruppenmitglieder

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/group

- Vier Spalten getrennt durch „:“
- Gruppenname, Passwort, Gruppen-ID, Gruppenmitglieder

/etc/group

```
root:x:0:
...
floppy:x:19:
games:x:20:
tape:x:21:
cdrom:x:22:
...
usb:x:43:
cdwriter:x:80:
audio:x:81:
video:x:82:
dialout:x:83:
users:x:100:
...
oli:x:10001:
...
```

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/shadow

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/shadow

- Neun Spalten getrennt durch „:“

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/shadow

- Neun Spalten getrennt durch „:“
- Benutzername, verschlüsseltes Passwort, letztes Änderungsdatum, minimales Passwortalter, maximales Passwortalter, Warnungszeitraum, Inaktivitätszeitraum, Zugangsverfallsdatum, reserviertes Feld

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

/etc/shadow

- Neun Spalten getrennt durch „:“
- Benutzername, verschlüsseltes Passwort, letztes Änderungsdatum, minimales Passwortalter, maximales Passwortalter, Warnungszeitraum, Inaktivitätszeitraum, Zugangsverfallsdatum, reserviertes Feld

/etc/shadow

```
oli:$2a$08$qzAg4PysVzQ/UdBxsrJtoeQbwLiraSshVN8b/WJviAkCatjSMIV7e:15180:0:99999:7:::
```

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

- Verschlüsselung mit Hilfe der *crypt*-Funktion

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

- Verschlüsselung mit Hilfe der *crypt*-Funktion
- Früher DES

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

- Verschlüsselung mit Hilfe der *crypt*-Funktion
- Früher DES - nur 8 Zeichen Passwortlänge

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

- Verschlüsselung mit Hilfe der *crypt*-Funktion
- Früher DES - nur 8 Zeichen Passwortlänge
- Passwort geht in Key-Generierung ein, Verschlüsselung eines Strings aus Nullen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

- Verschlüsselung mit Hilfe der *crypt*-Funktion
- Früher DES - nur 8 Zeichen Passwortlänge
- Passwort geht in Key-Generierung ein, Verschlüsselung eines Strings aus Nullen
- In */etc/shadow* wird verschlüsselter Text gespeichert

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

- Verschlüsselung mit Hilfe der *crypt*-Funktion
- Früher DES - nur 8 Zeichen Passwortlänge
- Passwort geht in Key-Generierung ein, Verschlüsselung eines Strings aus Nullen
- In */etc/shadow* wird verschlüsselter Text gespeichert
- Heute üblicherweise blowfish-basiert

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Passwortverschlüselung

- Verschlüsselung mit Hilfe der *crypt*-Funktion
- Früher DES - nur 8 Zeichen Passwortlänge
- Passwort geht in Key-Generierung ein, Verschlüsselung eines Strings aus Nullen
- In */etc/shadow* wird verschlüsselter Text gespeichert
- Heute üblicherweise blowfish-basiert - 72 Zeichen Passwortlänge

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Dateirechte

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Dateirechte

- Drei Bytes für Dateirechte, Darstellung numerisch oder über Angaben für Lesen, Schreiben und Ausführen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Dateirechte

- Drei Bytes für Dateirechte, Darstellung numerisch oder über Angaben für Lesen, Schreiben und Ausführen
- Erstes Byte für den Eigentümer, zweites für die Gruppe, drittes für andere

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Dateirechte

- Drei Bytes für Dateirechte, Darstellung numerisch oder über Angaben für Lesen, Schreiben und Ausführen
- Erstes Byte für den Eigentümer, zweites für die Gruppe, drittes für andere
- Dateisystem muss dies unterstützen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Dateirechte

- Drei Bytes für Dateirechte, Darstellung numerisch oder über Angaben für Lesen, Schreiben und Ausführen
- Erstes Byte für den Eigentümer, zweites für die Gruppe, drittes für andere
- Dateisystem muss dies unterstützen
  heute: ext-Familie Standard

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Dateirechte

- Drei Bytes für Dateirechte, Darstellung numerisch oder über Angaben für Lesen, Schreiben und Ausführen
- Erstes Byte für den Eigentümer, zweites für die Gruppe, drittes für andere
- Dateisystem muss dies unterstützen
  heute: ext-Familie Standard
  früher: xfs, jfs, reiserfs

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Dateirechte

- Drei Bytes für Dateirechte, Darstellung numerisch oder über Angaben für Lesen, Schreiben und Ausführen
- Erstes Byte für den Eigentümer, zweites für die Gruppe, drittes für andere
- Dateisystem muss dies unterstützen
  heute: ext-Familie Standard
  früher: xfs, jfs, reiserfs

Dateirechte

```
drwxr-xr-x 5 oli oli 4096 Nov 21 13:25 latex/
```

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Erweiterte Rechteverwaltung

DHBW Stuttgart
Duale Hochschule
Baden-Württemberg

Erweiterte Rechteverwaltung

- Normales Berechtigungssystem ist starr

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Erweiterte Rechteverwaltung

- Normales Berechtigungssystem ist starr
- Teilweise existiert die Notwendigkeit, mehreren Benutzern Rechte einzuräumen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Erweiterte Rechteverwaltung

- Normales Berechtigungssystem ist starr
- Teilweise existiert die Notwendigkeit, mehreren Benutzern Rechte einzuräumen
- Vorgehensweise über den *Extended Access Control Layer*

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Erweiterte Rechteverwaltung

- Normales Berechtigungssystem ist starr
- Teilweise existiert die Notwendigkeit, mehreren Benutzern Rechte einzuräumen
- Vorgehensweise über den *Extended Access Control Layer*
- Systembefehle *setfacl* und *getfacl*

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Erweiterte Rechteverwaltung

- Normales Berechtigungssystem ist starr
- Teilweise existiert die Notwendigkeit, mehreren Benutzern Rechte einzuräumen
- Vorgehensweise über den *Extended Access Control Layer*
- Systembefehle *setfacl* und *getfacl*

setfacl

```
setfacl -m u:lisa:r file
```

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Zugriff auf Systemressourcen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Zugriff auf Systemressourcen

- Früher: Ressource gehörte *root* und einer Gruppe.

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Zugriff auf Systemressourcen

- Früher: Ressource gehörte *root* und einer Gruppe.
- Benutzer mussten Mitglieder entsprechender Gruppe sein.

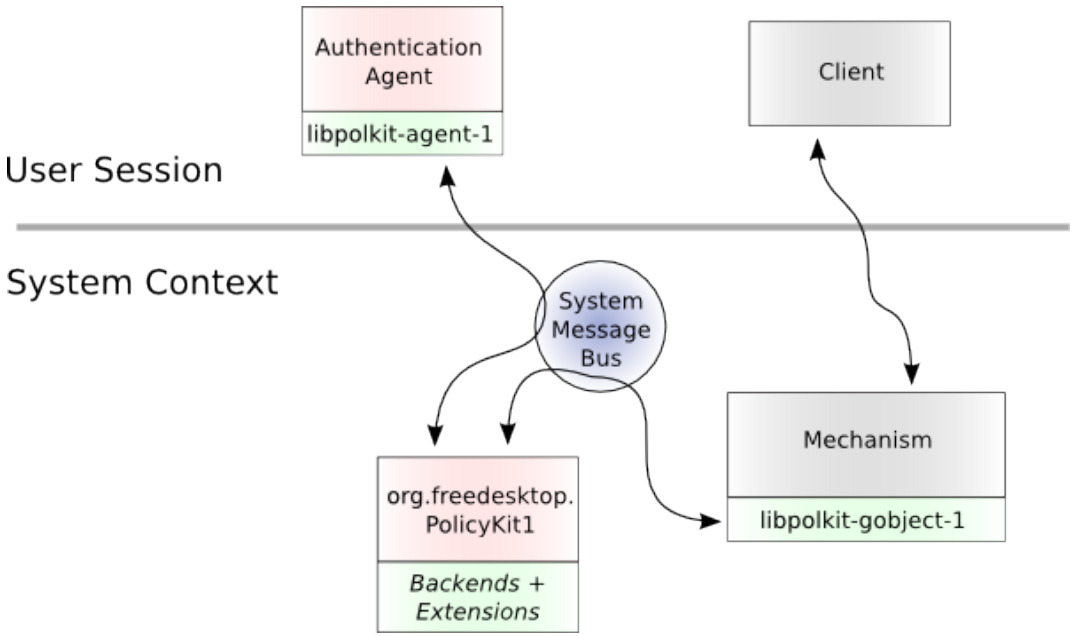
DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Zugriff auf Systemressourcen

- Früher: Ressource gehörte *root* und einer Gruppe.
- Benutzer mussten Mitglieder entsprechender Gruppe sein.
- Heute: *Policykit*

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Policykit



DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Was kommt?

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Was kommt?

- Systemunterbau im Umbruch:

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Was kommt?

- Systemunterbau im Umbruch:
  - *HAL* entfällt

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Was kommt?

- Systemunterbau im Umbruch:
  - *HAL* entfällt
  - *Policykit* wird reimplementiert

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Was kommt?

- Systemunterbau im Umbruch:
  - *HAL* entfällt
  - *Policykit* wird reimplementiert
  - ...

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Windows

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Windows

- Am meisten verbreitetes Desktop-Betriebssystem...

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Windows

- Am meisten verbreitetes Desktop-Betriebssystem...
- ...dadurch attraktivste Plattform für Angreifer

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Windows

- Am meisten verbreitetes Desktop-Betriebssystem...
- ...dadurch attraktivste Plattform für Angreifer
- Folge: Microsoft fügt mit jeder Windows-Version neue Sicherheitsmechanismen hinzu

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS - „New Technology File System“

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS - „New Technology File System“

- Ab Windows NT verfügbar

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS - „New Technology File System“

- Ab Windows NT verfügbar
- Standard Dateisystem ab Windows 2000

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS - „New Technology File System“

- Ab Windows NT verfügbar
- Standard Dateisystem ab Windows 2000
- Windows 9x wird nicht unterstützt

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Verbesserungen gegenüber FAT

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Verbesserungen gegenüber FAT

- Metadaten-Journaling: automatische Korrektur des Dateisystems
  Achtung: Daten selbst können nicht korrigiert werden!

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Verbesserungen gegenüber FAT

- Metadaten-Journaling: automatische Korrektur des Dateisystems
  Achtung: Daten selbst können nicht korrigiert werden!
- Verwendung langer Dateinamen (255 Zeichen) und Pfade (32767 Zeichen)

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Verbesserungen gegenüber FAT

- Metadaten-Journaling: automatische Korrektur des Dateisystems
  Achtung: Daten selbst können nicht korrigiert werden!
- Verwendung langer Dateinamen (255 Zeichen) und Pfade (32767 Zeichen)
- Dateigrößenbeschränkung von 4GB auf 16EiB angehoben (theor. Wert)

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Verbesserungen gegenüber FAT

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Verbesserungen gegenüber FAT

- ACL-basiertes Berechtigungssystem für Dateien und Ordner

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Verbesserungen gegenüber FAT

- ACL-basiertes Berechtigungssystem für Dateien und Ordner
- Einfache Zugriffsrechte:
  - Vollzugriff, Ändern, Ordnerinhalt anzeigen
  - Lesen und Ausführen, Lesen, Schreiben

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Funktionen von NTFS

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Funktionen von NTFS

- Datenkompression

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Funktionen von NTFS

- Datenkompression
- EFS - Encrypting File System

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Funktionen von NTFS

- Datenkompression
- EFS - Encrypting File System
  - Verschlüsselung basiert auf DES

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Funktionen von NTFS

- Datenkompression
- EFS - Encrypting File System
  - Verschlüsselung basiert auf DES
  - Keine User-Interaktion benötigt

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Funktionen von NTFS

- Datenkompression
- EFS - Encrypting File System
  - Verschlüsselung basiert auf DES
  - Keine User-Interaktion benötigt
  - Berechtigen von weiteren Usern auf verschlüsselte Daten

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS-Berechtigungskonzept

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS-Berechtigungskonzept

- Jedes Objekt im Dateisystem hat einen Security Descriptor (SD)

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS-Berechtigungskonzept

- Jedes Objekt im Dateisystem hat einen Security Descriptor (SD)
- SD arbeitet mit zwei ACLs

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS-Berechtigungskonzept

- Jedes Objekt im Dateisystem hat einen Security Descriptor (SD)
- SD arbeitet mit zwei ACLs
  - Discretionary ACL - legt fest, welche Benutzer/Gruppen Zugriff haben

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS-Berechtigungskonzept

- Jedes Objekt im Dateisystem hat einen Security Descriptor (SD)
- SD arbeitet mit zwei ACLs
  - Discretionary ACL - legt fest, welche Benutzer/Gruppen Zugriff haben
  - System ACL - legt u.a. fest, welche Zugriffe vom System protokolliert werden

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS-Berechtigungskonzept

- Jedes Objekt im Dateisystem hat einen Security Descriptor (SD)
- SD arbeitet mit zwei ACLs
  - Discretionary ACL - legt fest, welche Benutzer/Gruppen Zugriff haben
  - System ACL - legt u.a. fest, welche Zugriffe vom System protokolliert werden
- Zur Einsparung von Speicherplatz wird Hash von SD gebildet

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

NTFS-Berechtigungskonzept

- Jedes Objekt im Dateisystem hat einen Security Descriptor (SD)
- SD arbeitet mit zwei ACLs
  - Discretionary ACL - legt fest, welche Benutzer/Gruppen Zugriff haben
  - System ACL - legt u.a. fest, welche Zugriffe vom System protokolliert werden
- Zur Einsparung von Speicherplatz wird Hash von SD gebildet
- Objekte mit identischem “Hash(SD)“ verweisen auf denselben SD

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

- Eingeführt mit Windows Vista

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

- Eingeführt mit Windows Vista
- Soll Integrität des Betriebssytems sicherstellen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

- Eingeführt mit Windows Vista
- Soll Integrität des Betriebssytems sicherstellen
- Klassifizierung der auf Objekte [1] zugreifenden Subjekte [2] via Integritäts-Level

[1] Alle zugreifbaren Objekte
[2] Benutzer, Prozesse, Dienste

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

- Eingeführt mit Windows Vista
- Soll Integrität des Betriebssytems sicherstellen
- Klassifizierung der auf Objekte [1] zugreifenden Subjekte [2] via Integritäts-Level
- Greift noch vor DACL-Abfragen

[1] Alle zugreifbaren Objekte
[2] Benutzer, Prozesse, Dienste

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

DHBW Stuttgart
Duale Hochschule
Baden-Württemberg

Mandatory Integrity Control

- Vereinfachtes Biba-Modell

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

- Vereinfachtes Biba-Modell
- Per Default nur No-Write-Up

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Mandatory Integrity Control

- Vereinfachtes Biba-Modell
- Per Default nur No-Write-Up
- Dient v.a. dem Schutz der Systemdateien

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Integritäts-Level (IL)

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Integritäts-Level (IL)

- untrusted - wird i.d.R. nicht verwendet

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Integritäts-Level (IL)

- untrusted - wird i.d.R. nicht verwendet
- low - temporäre Internetdateien, IE im protected mode

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Integritäts-Level (IL)

- untrusted - wird i.d.R. nicht verwendet
- low - temporäre Internetdateien, IE im protected mode
- medium - IL der Standardbenutzer

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Integritäts-Level (IL)

- untrusted - wird i.d.R. nicht verwendet
- low - temporäre Internetdateien, IE im protected mode
- medium - IL der Standardbenutzer
- high - IL der Administratoren

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Integritäts-Level (IL)

- untrusted - wird i.d.R. nicht verwendet
- low - temporäre Internetdateien, IE im protected mode
- medium - IL der Standardbenutzer
- high - IL der Administratoren
- system - Ausschließlich für system-/kernelnahe Prozesse und Dienste

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Speicherung des IL

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Speicherung des IL

- Subjekte erhalten zusätzlichen Security-ID-Wert im Anmeldungstoken
- Beispiele: Jeder S-1-1-0; aufer S-1-1-8192

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

MIC - Speicherung des IL

- Subjekte erhalten zusätzlichen Security-ID-Wert im Anmeldungstoken
- Beispiele: Jeder S-1-1-0; aufer S-1-1-8192
- Objekte speichern IL in SACL des Security Descriptors

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Sicherheitsmechanismen

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Weitere Sicherheitsmechanismen

- Systemprivilegien
- Data Execution Prevention (ab XP)
- User Account Control (ab Vista)
- Address Space Layout Randomization

DHBW Stuttgart
Duale Hochschule Baden-Württemberg

Vielen Dank!

Noch Fragen?

DHBW Stuttgart
Duale Hochschule Baden-Württemberg