AK-Treffen „Mobile Datenbanken und Informationssysteme“

Aspekte der Datensicherheit in mobilen Datenbanken

Thomas Fanghänel

thf@informatik.uni-jena.de

Friedrich-Schiller-Universität Jena
Institut für Informatik
Lehrstuhl für Datenbanken und Informationssysteme

Jena, Thüringen *23. November 2001*

Gliederung

1. Motivation
2. Konzepte und Techniken der Datenbanksicherheit im mobilen Kontext
3. Am Beispiel: Prototypisches Sicherheitskonzept für DB2 Everyplace
4. Zusammenfassung und Ausblick

Motivation

- Mobile Endgeräte (Handhelds, PDAs, Organizer) finden immer mehr Einsatz im Unternehmensumfeld.
- Tendenz zu mobilen Versionen von Unternehmenssoftware ist erkennbar.
- Nutzung von zentral gehaltenen Unternehmensdaten auf mobilem Endgerät notwendig.

$\Rightarrow$ **Mobile Datenbanksysteme**

Aber:

- Hochsensible Unternehmensdaten auf wenig gesicherten Endgeräten sind ein Risiko.
- Weit verbreitete mobile Endgeräte bieten nahezu keine Sicherheitsfunktionen.

Sicherheitsanforderungen, wie man sie bei zentralen Datenbankservern stellt (und umsetzt), müssen in geeigneter Weise auch für mobile Datenbanken umgesetzt werden können.

Gefahren für die Datensicherheit und Techniken zur Gefahrenvermeidung

- Unautorisierte Zugriffe, Manipulationen, Löschungen von Daten gefährden Datenintegrität und -sicherheit.
- Gefährdung kann zufällig auftreten oder vorsätzlich herbeigeführt werden.
- Vorsätzlich herbeigeführte Gefährdungen können von autorisierten oder nicht autorisierten Nutzern hervorgerufen werden.

Ein Sicherheitskonzept für ein DBMS soll vorsätzliche Gefährdungen der Datensicherheit verhindern.

- Unterschiedliche Ebenen für Sicherheitsvorkehrungen denkbar: Nutzerebene, Geräteebene, Betriebssystemebene, Netzwerkebene, DBMS-Ebene.
- Mögliche Vorkehrungen unterscheiden sich für mobile und nicht-mobile Datenbanksysteme und Umgebungen. Besonders: Geräteebene, Betriebssystemebene.

Sicherheitskonzept eines mobilen DBMS muß an mobile Umgebungsbedingungen angepaßt werden.

Schutzziele und -techniken

Schutzziele:

- *Vertraulichkeit* – Nur autorisierte Nutzer dürfen auf Daten zugreifen.
- *Integrität* – Nur autorisierte Nutzer dürfen Daten ändern, und zwar nur auf autorisierte Art und Weise.
- *Verbindlichkeit* – Informationen über Zugriffe und zugreifende Nutzer müssen verfügbar und Änderungen an Daten müssen autorisierten Nutzern zuordenbar sein.
- *Verfügbarkeit* – Autorisierte Nutzer können jederzeit auf die Daten zugreifen.

Schutztechniken:

- *Nutzerauthentifizierung* – Eindeutige positive Identifizierung von Nutzern, nötig für Umsetzung von Auditability und Zugriffskontrollmechanismen.
- *Zugriffskontrollmechanismen* – Rechtevergabe an Nutzer für einzelne Objekte oder Zuordnung von Zugriffsstufen an Objekte.
- *Verschlüsselung* – Möglicher Einsatz zur Sicherung der Vertraulichkeit von Daten und zum Schutz vor unautorisierten Datenzugriffen unter Umgehung des DBMS.

Prototypisches Sicherheitskonzept für IBM DB2 Everyplace

Anforderungen:

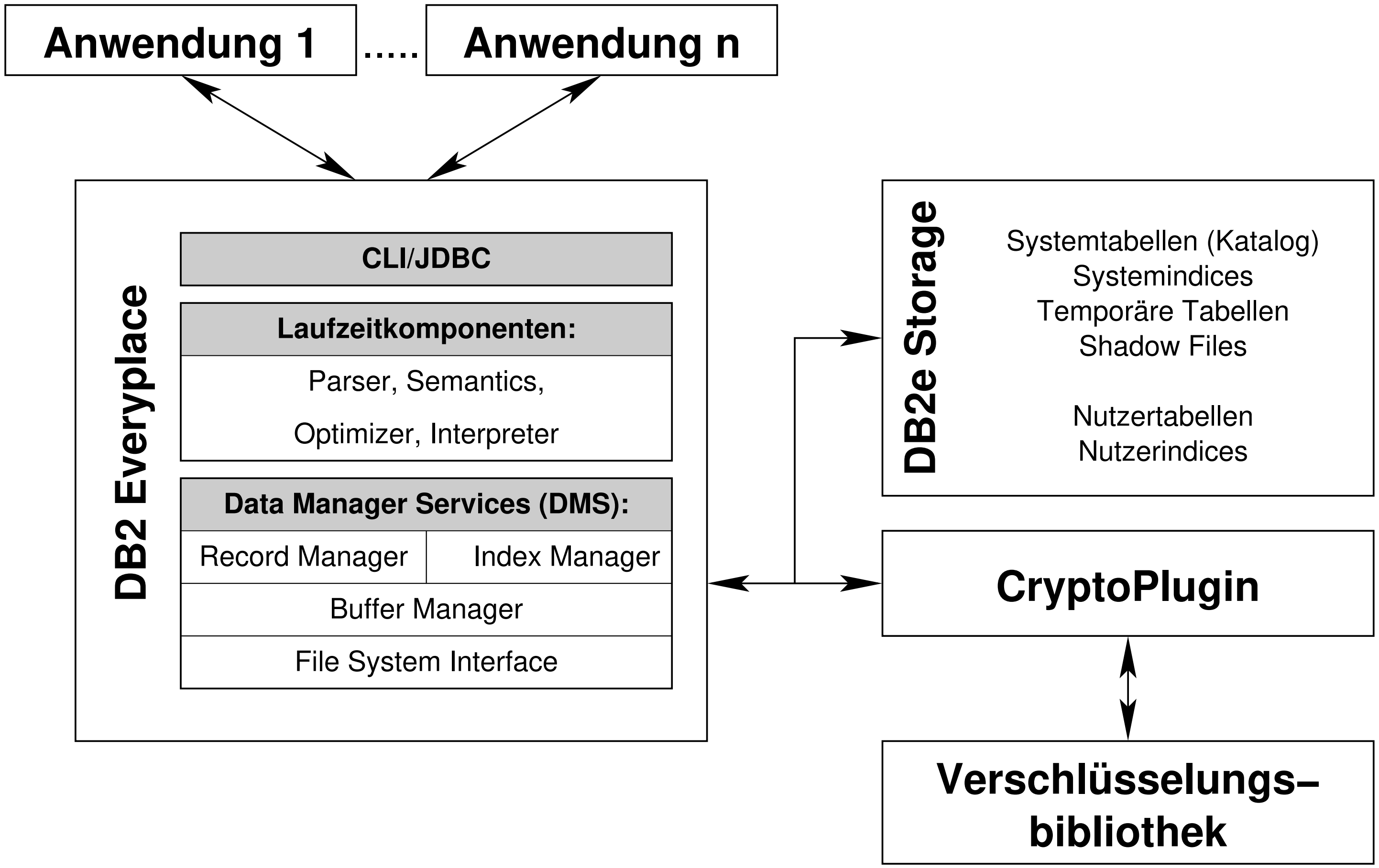
- Optionale Datenverschlüsselung für DB2e-Tabellen.
- Minimale Änderungen an der bestehenden Architektur von DB2e.
- Minimale Performance-Einbußen und Vergößerung des Programmcodes..
- Keine Beeinträchtigung der Datenbankfunktionalität (z. B. Indexnutzung).
- Keine Abkehr vom *zero administration*-Prinzip fuer den mobilen Datenbank-Client.
- Leichte Austauschbarkeit des Verschlüsselungsalgorithmus.

Lösung: Verschlüsselungsfunktionalität als Kernel-Plugin.

Seiteneffekte:

- Entwicklung eines Nutzer(authentifizierungs)konzeptes notwendig.

Aufbau von DB2 Everyplace



Reichweite und Granularität für die Verschlüsselung von Daten

Was wird verschlüsselt?

- Verschlüsselung für Nutzertabellen als Option (`CREATE TABLE ... WITH ENCRYPTION`).
- Keine Verschlüsselung für Metadaten- (Katalogtabellen-) und Indexdateien.
- Bedingte Verschlüsselung für temporäre Tabellen und *shadow files*.

Welche Granularität wird für die Verschlüsselung gewählt?

- Mögliche Granularitäten sind globale Verschlüsselung bzw. Datenbank, Tabelle, Spalte, Record oder Attributwert. Physische Granulate nicht geeignet für Verschlüsselung.
- Aus Performance-Gründen scheiden globale Verschlüsselung sowie Verschlüsselung auf Datenbank-Ebene aus.

Implementierungsaspekte

Wo werden Verschlüsselungsoperationen innerhalb des Kerns durchgeführt?

- *File System Interface* – Arbeitet mit Seiten fixer Größe, Verschlüsselungsoperationen während des Lesens bzw. Schreibens einer Seite. Implementierung von Verschlüsselung auf Tabellenbasis oder gröberer Granularität möglich.

- *Buffer Manager* – Arbeitet mit Seiten fixer Größe, Ver-/Entschlüsselung während des Lesens oder Schreibens aus/in eine Seite. Ebenfalls nur Tabellen oder gröbere Granulate für Verschlüsselung möglich.

- *Record Manager* – Arbeitet mit Records variabler Länge, Verschlüsselungsoperationen während des (Ent-)Packens eines Records. Granulate auch unterhalb von Tabellen möglich.

Entscheidung für Implementierung auf FS-Ebene wegen geringster zu erwartender Anzahl an Ver-/Entschlüsselungsoperationen. Dadurch auch Festlegung auf Tabellengranulat.

Weitere Eigenschaften und erreichte Ziele

Weitere Eigenschaften des Prototyps:

- Nutzerauthentifizierungs- und Schlüsselverwaltungmechanismen benutzen ebenfalls Plugin-Funktionen.
- Nutzerverwaltung und Zugriff auf verschlüsselte Daten geschieht für den Endnutzer nahezu transparent.
- SyncServer unterstützt Synchronisation von verschlüsselten Tabellen.

Bewertung und Einordnung des Prototyps:

- Schutz der Vertraulichkeit der Daten wird vom mobilen DBMS übernommen.
- Verschlüsselungsansatz erhöht nur die Vertraulichkeit der Daten, nicht die Integrität.
- (Noch) Keinerlei Mechanismen zur Sicherung der Verbindlichkeit der Daten.

Zusammenfassung und Ausblick

Zusammenfassung:

- Untersuchung und Klassifizierung von Sicherheitsaspekten im Kontext mobiler Datenbanken.
- Praktische Umsetzung einzelner Lösungsansätze in Form einer prototypischen Sicherheitsinfrastruktur für DB2 Everyplace.

Weitere Arbeiten:

- Funktionale Erweiterungen des existierenden Prototyps.
- Verfeinerung des existierenden Prototyps hin zu differenzierteren Nutzerprivilegien.
- Vergleichende Messungen und Benchmarks bei Nutzung verschlüsselter und unverschlüsselter Tabellen.
- Auswirkung auf Cache- und Optimierungsstrategien, Entwicklung von Alternativen.
- Produktintegration.

Vielen Dank!