

Datenbanken und Datensicherheit

Prof. Dr. rer. nat. Peter Gerwinski

18. Januar 2024

Datenbanken und Datensicherheit

<https://gitlab.cvh-server.de/pgerwinski/dbs>

- 1 Einführung**
- 2 Kurzeinführung Unix**
- 3 Kurzeinführung TCP/IP**
- 4 Relationale Datenbanken**
 - ...
 - 4.11 GUI-Zugriff
 - 4.12 SQL Injection
 - 4.13 Datensicherheit bei Datenbanken
 - 4.14 Sonstige Datenbanken
- 5 Kryptographie**
 - 5.1 Einführung
 - 5.2 Symmetrische Verschlüsselung
 - 5.3 Asymmetrische Verschlüsselung
 - 5.4 Signaturen
 - ...
- 6 Netzwerksicherheit**
- 7 Verfügbarkeit**
- 8 Datenschutz**



Änderungen
vorbehalten

4 Relationale Datenbanken

4.11 SQL Injection

Problem:

- Ein böswilliger Benutzer gibt über eine Benutzerschnittstelle (z. B. ein Web-Interface) Daten ein (z. B. einen „Namen“), die Sonderzeichen enthalten, damit sie als SQL-Befehle ausgeführt werden.
- Literatur: <https://xkcd.com/327/>

Lösung: Die Benutzerschnittstelle prüft die Daten auf Sonderzeichen und ersetzt diese durch geeignete Escape-Sequenzen

- ' durch '' ersetzen
- Funktion `CHR ()`
- Viele DBMS verstehen ein vorangestelltes \.

Bessere Lösung: *Prepared Statements*

- <https://www.postgresql.org/docs/current/sql-prepare.html>
- https://www.w3schools.com/php/php_mysql_prepared_statements.asp

4 Relationale Datenbanken

4.12 Datensicherheit bei Datenbanken

- kein direkter Zugriff von außen auf die Datenbank
- feingranulare Benutzerrechte
- Software aktuell halten
- Prepared Statements
- Transportverschlüsselung

4 Relationale Datenbanken

4.13 Sonstige Datenbanken

- Eingebettete Datenbanken:
Berkeley DB, SQLite
Software-Bibliothek, keine Client-Server-Struktur
- Nicht-relationale Datenbanken:
dokumentenorientierte Datenbanken, noSQL
Performanz wichtiger als Konsistenz
→ Applikationen stärker in Konsistenzprüfung eingebunden

5 Kryptographie

5.1 Einführung

Was ist Datensicherheit?

(CIA)

- Vertraulichkeit (confidentiality) → Verschlüsselung
- Integrität (integrity) → Konsistenzprüfungen, Prüfwerte, Signaturen
- Verfügbarkeit (availability) → Backups, Ausfallsicherheit

- Identifizierbarkeit (Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit)
→ Passwörter, Signaturen
bzw.
- Anonymität (plausible Abstreitbarkeit, Nichtzurechenbarkeit)
→ Pseudonymisierung, Anonymisierung,
Verschlüsselung, Steganographie

5 Kryptographie

5.1 Einführung

Was ist Datensicherheit?

- (CIA)
- Vertraulichkeit (confidentiality) → **Verschlüsselung**
- Integrität (integrity) → Konsistenzprüfungen, Prüfwerte, **Signaturen**
- Verfügbarkeit (availability) → Backups, Ausfallsicherheit
- Identifizierbarkeit (Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit)
→ **Passwörter, Signaturen**
bzw.
- Anonymität (plausible Abstreitbarkeit, Nichtzurechenbarkeit)
→ Pseudonymisierung, Anonymisierung,
Verschlüsselung, Steganographie → **Kryptographie**

5 Kryptographie

Kryptographie

- Verschlüsselung: symmetrisch, asymmetrisch, hybrid
- Hashes: Einwegfunktionen, Salt
- Signaturen, Zertifikate
- Schlüsselaustausch

5.2 Symmetrische Verschlüsselung

- Derselbe Schlüssel zum Ver- und Entschlüsseln
- Beispiele: Cäsar-Chiffre, Monoalphabetische Substitution

5 Kryptographie

Kryptographie

- Verschlüsselung: symmetrisch, asymmetrisch, hybrid
- Hashes: Einwegfunktionen, Salt
- Signaturen, Zertifikate
- Schlüsselaustausch

5.2 Symmetrische Verschlüsselung

- Derselbe Schlüssel zum Ver- und Entschlüsseln
- Beispiele: Cäsar-Chiffre, Monoalphabetische Substitution, One Time Pad

5 Kryptographie

Kryptographie

- Verschlüsselung: symmetrisch, asymmetrisch, hybrid
- Hashes: Einwegfunktionen, Salt
- Signaturen, Zertifikate
- Schlüsselaustausch

5.2 Symmetrische Verschlüsselung

- Derselbe Schlüssel zum Ver- und Entschlüsseln
- Beispiele: Cäsar-Chiffre, Monoalphabetische Substitution, One Time Pad

- Problem: Schlüsselaustausch

5 Kryptographie

Kryptographie

- Verschlüsselung: symmetrisch, asymmetrisch, hybrid
- Hashes: Einwegfunktionen, Salt
- Signaturen, Zertifikate
- Schlüsselaustausch

5.2 Symmetrische Verschlüsselung

- Derselbe Schlüssel zum Ver- und Entschlüsseln
- Beispiele: Cäsar-Chiffre, Monoalphabetische Substitution, One Time Pad, Pseudozufallszahlengenerator, Startwert als Schlüssel
- Problem: Schlüsselaustausch

5 Kryptographie

Kryptographie

- Verschlüsselung: symmetrisch, asymmetrisch, hybrid
- Hashes: Einwegfunktionen, Salt
- Signaturen, Zertifikate
- Schlüsselaustausch

5.2 Symmetrische Verschlüsselung

- Derselbe Schlüssel zum Ver- und Entschlüsseln
- Beispiele: Cäsar-Chiffre, Monoalphabetische Substitution, One Time Pad, *spezielle* Pseudozufallszahlengeneratoren, Startwert als Schlüssel: Enigma, DES, 3DES, RC4, IDEA, Blowfish, TwoFish, CAST, AES, ...
- Problem: Schlüsselaustausch

5 Kryptographie

Kryptographie

- Verschlüsselung: symmetrisch, asymmetrisch, hybrid
- Hashes: Einwegfunktionen, Salt
- Signaturen, Zertifikate
- Schlüsselaustausch

5.2 Symmetrische Verschlüsselung

- Derselbe Schlüssel zum Ver- und Entschlüsseln
- Beispiele: Cäsar-Chiffre, Monoalphabetische Substitution, One Time Pad, *spezielle* Pseudozufallszahlengeneratoren, Startwert als Schlüssel: Enigma, DES, 3DES, RC4, IDEA, Blowfish, TwoFish, CAST, AES, ...
- Problem: Schlüsselaustausch

5 Kryptographie

Kryptographie

- Verschlüsselung: symmetrisch, asymmetrisch, hybrid
- Hashes: Einwegfunktionen, Salt
- Signaturen, Zertifikate
- Schlüsselaustausch

5.2 Symmetrische Verschlüsselung

- Derselbe Schlüssel zum Ver- und Entschlüsseln
- Beispiele: **Cäsar-Chiffre**, **Monoalphabetische Substitution**, One Time Pad, *spezielle* Pseudozufallszahlengeneratoren, Startwert als Schlüssel: **Enigma**, **DES**, **3DES**, **RC4**, IDEA, Blowfish, TwoFish, CAST, AES, ...
- Problem: Schlüsselaustausch
- Lösung: *asymmetrische Verschlüsselung*

5.3 Asymmetrische Verschlüsselung

- verschiedene Schlüssel zum Ver- und Entschlüsseln:
öffentlicher und privater Schlüssel
- Prinzip: mathematische Operation,
einfach durchzuführen, schwer rückgängig zu machen
- Beispiel: $N = p \cdot q$ – einfacher als Primfaktorzerlegung von $N \longrightarrow$ RSA
 $73 \cdot 97 = 7081$: geht notfalls noch im Kopf
Primfaktorzerlegung von 7081: mindestens schriftlich, besser mit Rechner
- Beispiel: $c = b^a$ – einfacher als $a = \log_b c \longrightarrow$ Diffie-Hellman, ElGamal
 $7^5 = 16807$: geht notfalls noch im Kopf
 $\log_7 16807$: mindestens schriftlich, besser mit Rechner

→ Details: Algorithmen und Datenstrukturen

5.3 Asymmetrische Verschlüsselung

- verschiedene Schlüssel zum Ver- und Entschlüsseln:
öffentlicher und privater Schlüssel
- Prinzip: mathematische Operation,
einfach durchzuführen, schwer rückgängig zu machen
- Beispiel: $N = p \cdot q$ – einfacher als Primfaktorzerlegung von $N \longrightarrow$ RSA
 $73 \cdot 97 = 7081$: geht notfalls noch im Kopf
Primfaktorzerlegung von 7081: mindestens schriftlich, besser mit Rechner
- Beispiel: $c = b^a$ – einfacher als $a = \log_b c \longrightarrow$ Diffie-Hellman, ElGamal
 $7^5 = 16807$: geht notfalls noch im Kopf
 $\log_7 16807$: mindestens schriftlich, besser mit Rechner

→ Details: Algorithmen und Datenstrukturen

- Nachteil: wesentlich aufwendiger und daher langsamer
als symmetrische Verschlüsselung

→ *hybride Verschlüsselung*: nur Schlüsselaustausch asymmetrisch,
eigentliche Verschlüsselung symmetrisch

5.4 Signaturen

- *kryptographische Hash-Funktion*: leicht auszurechnen, schwer zu manipulieren
- asymmetrisch: *Signatur*
Hash-Wert mit privatem Schlüssel verschlüsseln,
mit öffentlichem Schlüssel entschlüsseln
- symmetrisch: *Message Authentication Code* (MAC)
z. B. Hash-Wert über Nachricht + geheimer Schlüssel

5.4 Signaturen

- *kryptographische Hash-Funktion*: leicht auszurechnen, schwer zu manipulieren
- asymmetrisch: *Signatur*
Hash-Wert mit privatem Schlüssel verschlüsseln,
mit öffentlichem Schlüssel entschlüsseln
- symmetrisch: *Message Authentication Code* (MAC)
z. B. Hash-Wert über Nachricht + geheimer Schlüssel

Angriffsmöglichkeit: *Man-in-the-middle*-Angriff

Beim Schlüsselaustausch anderen Schlüssel unterschieben

→ Sorgfalt beim Schlüsselaustausch

5.4 Signaturen

- *kryptographische Hash-Funktion*: leicht auszurechnen, schwer zu manipulieren
- asymmetrisch: *Signatur*
Hash-Wert mit privatem Schlüssel verschlüsseln,
mit öffentlichem Schlüssel entschlüsseln
- symmetrisch: *Message Authentication Code* (MAC)
z. B. Hash-Wert über Nachricht + geheimer Schlüssel

Angriffsmöglichkeit: *Man-in-the-middle*-Angriff

Beim Schlüsselaustausch anderen Schlüssel unterchieben

→ Sorgfalt beim Schlüsselaustausch

Praxis-Beispiele

- SSH
- HTTPS
- OpenPGP

5.5 Authentifizierung

- Zugangsdaten:
Benutzername, Passwort
- Problem:
Zugangsdaten mitlesen
- Lösung:
verschlüsselte Verbindung
- Problem:
Zugangsdaten speichern
- Lösung:
Hash-Wert statt Passwort
speichern
- Problem:
gleiche Passwörter identifizierbar
- Lösung:
Salt

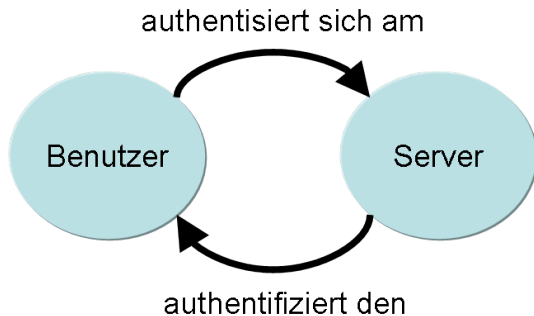


Bild: <https://de.wikipedia.org/wiki/Datei:Authentisieren-authentifizieren.png>

5.5 Authentifizierung

- Zugangsdaten:
Benutzername, Passwort
- Problem:
Zugangsdaten mitlesen
- Lösung:
verschlüsselte Verbindung
- Lösung:
Challenge-Response-Authentifizierung
Beispiel: HTTP Digest

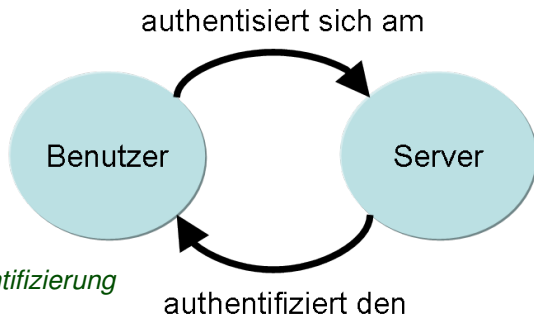


Bild: <https://de.wikipedia.org/wiki/Datei:Authentisieren-authentifizieren.png>

- gemeinsamer geheimer Schlüssel (Passwort)
- Server schickt *Nonce* an Benutzer
- Benutzer schickt Hash über [Passwort + Nonce] an Server
- Server berechnet denselben Hash → Authentifizierung erfolgreich
- Nonce nur einmal verwenden!
(„number used once“)

5.6 Quantencomputer

- Prinzip: 2^n Berechnungen gleichzeitig
(n = Registerbreite)

—> Klassisch schwierige Probleme werden einfacher.

- Beispiel: Primfaktorzerlegung: $\mathcal{O}(n^3)$ statt $\mathcal{O}(2^{\sqrt{n \log n}})$
- Problem für asymmetrische Verschlüsselungsalgorithmen,
z. B. RSA (Primfaktorzerlegung), ElGamal (diskreter Logarithmus)
- weniger problematisch für symmetrische Verschlüsselungsalgorithmen

—> Suche nach Post-Quanten-Kryptographie
Beispiel: McEliece-Kryptosystem

—> *Forward Secrecy*

Kompromittierung betrifft nur zukünftige Kommunikation,
nicht bereits vergangene. Beispiel:

- RSA nur für Authentifizierung
- Austausch eines Sitzungsschlüssels via Diffie-Hellman
- Kommunikation über Sitzungsschlüssel (symmetrisch)
- Sitzungsschlüssel nur einmal verwenden!

6 Netzwerksicherheit

- Firewall: nur bestimmte IP-Adressen / Ports / Inhalte zulassen
- VPN: verschlüsselte Verbindung von Netzwerken über ansonsten unsichere Verbindung (Internet)
- *Intrusion Detection System*

Anonymität

- Beispiel: Tor – Zwiebel-Routing
 - Tor-Browser
 - Tails
- Beispiel: Corona-Warn-App

Cross-Site-Scripting

6 Netzwerksicherheit

Die menschliche Komponente

- Bequemlichkeit
- Social Engineering
 - *Phishing*
 - KI-Sprachmodelle

*Es gibt für jedes menschliche Problem
immer eine wohl bekannte Lösung -
sauber, einleuchtend, und falsch.*

Henry Louis Mencken, The Divine Afflatus, 1917
<https://de.wikiquote.org/wiki/Lösung>

7 Verfügbarkeit

Wann wird wirklich auf den Datentäger geschrieben?

- DBMS: Persistenz-Einstellungen
- *Write Ahead Log (WAL)*
Journaling-Dateisysteme
- *CAP-Theorem*

Daten sicher aufbewahren

- Backup
- RAID

Hochverfügbarkeit

- allgemein: *High-Availability-Cluster*
- speziell: Datenbank-Cluster: Replikation über mehrere Server

8 Datenschutz

- Schutz vor mißbräuchlicher Datenverarbeitung
- informationelle Selbstbestimmung
- Persönlichkeitsrecht
- Privatsphäre

Datenmißbrauch ermöglicht hohe Gewinne

—> viel Interesse an persönlichen Daten

—> „Datenschutz hemmt ~~den Fortschritt!~~“ die persönliche Bereicherung

- DSGVO