

KEAMANAN DATA AKSES DALAM PERANCANGAN PERANGKAT LUNAK

Mata Kuliah: Software Engineering



DOSEN: Yudhi Fajar Saputra, S.Kom., M.Sc

Pertemuan ke-

Topik Bahasan ke-

SEMESTER : 3/ TA. 2024-2025

KODE MK/SKS: MKP001/3 SKS

**PRODI INFORMATIKA/ILMU KOMPUTER
UNIVERSITAS WIDYA GAMA MAHAKAM SAMARINDA**

Nama Mata Kuliah : Software Engineering/Rekayasa Perangkat Lunak
Kode Mata Kuliah/SKS : MKP ____/3 SKS
Dosen : **Yudhi Fajar Saputra,**
Semester : **3/ 2024**
Hari Pertemuan / Jam : -
Tempat Pertemuan : **Ruang Kelas A.06**

Keamanan data akses dalam pengembangan perangkat lunak merupakan aspek penting yang dirancang untuk melindungi data dari akses, penggunaan, dan pengungkapan yang tidak sah. Ini mencakup berbagai strategi seperti autentikasi, otorisasi, enkripsi, dan audit akses yang berperan dalam memastikan integritas, kerahasiaan, serta ketersediaan data. Proses ini bertujuan untuk menjaga kepercayaan pengguna dan memastikan bahwa perangkat lunak mematuhi standar keamanan yang berlaku, seperti GDPR dan HIPAA, yang memberikan pedoman ketat untuk perlindungan data [1,2]. Berikut adalah aspek dan teknik keamanan data akses:

1. AUTENTIKASI (AUTHENTICATION)

Autentikasi adalah proses verifikasi identitas pengguna atau sistem sebelum memberikan akses ke data. Ini adalah langkah pertama dalam memastikan bahwa hanya pengguna yang memiliki izin dapat masuk ke dalam sistem. Berbagai metode autentikasi meliputi:

- 1) **Kata sandi dan PIN:** Metode dasar yang memerlukan kata sandi untuk otentikasi.
- 2) **Multi Factor Authentication (MFA):** Memerlukan dua atau lebih faktor, misalnya kombinasi antara kata sandi dan kode OTP
- 3) **Biometrik:** Menggunakan data biologis seperti sidik jari atau pengenalan wajah untuk verifikasi.
- 4) **Token atau Sertifikat Digital:** Penggunaan token atau sertifikat yang secara otomatis mengotentikasi pengguna pada saat masuk

2. OTORISASI (AUTHORIZATION)

Setelah autentikasi, otorisasi menentukan data dan tindakan yang dapat diakses oleh pengguna. Ini adalah proses kontrol akses yang memastikan bahwa pengguna hanya dapat mengakses data yang sesuai dengan peran dan izin mereka. Model kontrol akses umum meliputi:

- 1) **Role-Based Access Control (RBAC):** Pengguna diberi akses berdasarkan peran tertentu (misalnya admin, pengguna biasa).
- 2) **Attribute-Based Access Control (ABAC):** Akses diberikan berdasarkan atribut

tertentu dari pengguna, seperti lokasi, departemen, atau status kerja.

- 3) **Mandatory Access Control (MAC):** Menentukan izin akses berdasarkan kebijakan keamanan yang ketat dan dikelola oleh administrator sistem.

3. ENKRIPSI DATA (DATA ENCRYPTION)

Enkripsi melindungi data dengan mengubahnya menjadi bentuk yang tidak dapat dibaca tanpa kunci dekripsi yang benar. Ini memastikan bahwa meskipun data diakses atau dicuri, pihak yang tidak berwenang tidak dapat membacanya. Jenis enkripsi meliputi:

- 1) **Enkripsi Data dalam Perjalanan (Data in Transit Encryption):** Melindungi data saat sedang ditransfer, seperti SSL/TLS untuk komunikasi internet.
- 2) **Enkripsi Data yang Tersimpan (Data at Rest Encryption):** Melindungi data saat disimpan di database atau server, seperti enkripsi disk penuh (Full Disk Encryption) atau enkripsi tingkat database.
- 3) **Enkripsi End-to-End:** Melindungi data sepanjang jalur pengiriman, sehingga hanya pengirim dan penerima yang dapat membacanya.

4. AUDIT DAN PEMANTAUAN AKSES (ACCESS AUDIT AND MONITORING)

Pemantauan akses melibatkan pengawasan aktivitas pengguna dalam sistem untuk mendeteksi akses yang mencurigakan atau aktivitas tidak sah. Log audit digunakan untuk mencatat siapa yang mengakses data apa, kapan, dan bagaimana caranya. Elemen kunci dari pemantauan akses meliputi:

- 1) **Logging Aktivitas:** Mencatat semua aktivitas pengguna dan sistem untuk analisis selanjutnya.
- 2) **Sistem Deteksi Intrusi (IDS) dan Pencegahan Intrusi (IPS):** Alat yang memonitor dan mendeteksi upaya akses ilegal serta secara otomatis mengambil tindakan.
- 3) **Notifikasi Real-Time:** Memberi peringatan jika terdeteksi upaya akses yang mencurigakan, sehingga dapat diambil tindakan segera

5. MANAJEMEN HAK AKSES (ACCESS RIGHTS MANAGEMENT)

Manajemen hak akses memastikan pengguna hanya memiliki hak yang diperlukan sesuai dengan prinsip **least privilege** (hak akses sekecil mungkin). Ini meliputi:

- 1) **Pembatasan Akses:** Pengguna hanya mendapatkan akses yang benar-benar dibutuhkan untuk pekerjaannya.
- 2) **Kontrol Hak Sementara (Temporary Privilege Control):** Memberi hak akses sementara kepada pengguna untuk tugas khusus dan mencabutnya setelah selesai.

- 3) **Penghapusan Akses Lama (Orphaned Access Removal):** Menghapus akses dari pengguna yang telah meninggalkan organisasi atau tidak lagi memerlukan akses.

6. PENERAPAN KEAMANAN APLIKASI (APPLICATION SECURITY IMPLEMENTATION)

Keamanan aplikasi mencakup teknik dan alat yang dirancang untuk melindungi perangkat lunak dari celah keamanan dan ancaman dari luar. Beberapa teknik Keamanan aplikasi meliputi:

- 1) **Penerapan Protokol HTTPS:** Untuk melindungi data dalam transmisi dari serangan perantara.
- 2) **Pemindaian Kerentanan (Vulnerability Scanning):** Mengidentifikasi kerentanan dalam kode perangkat lunak.
- 3) **Pengujian Keamanan Aplikasi:** Melakukan pengujian penetrasi untuk memastikan bahwa aplikasi tidak rentan terhadap serangan.

7. BACKUP DAN PEMULIHAN (BACKUP AND RECOVERY)

Keamanan data akses juga melibatkan kemampuan untuk melakukan backup dan pemulihan data jika terjadi insiden keamanan. Proses backup harus dilakukan secara teratur untuk memastikan data selalu tersedia dan tidak hilang:

- 1) **Backup Berkala:** Backup data secara berkala untuk mencegah kehilangan informasi..
- 2) **Penyimpanan Offsite:** Menyimpan backup di lokasi yang berbeda untuk menghindari risiko fisik..
- 3) **Pengujian Pemulihan:** Menguji rencana pemulihan untuk memastikan data dapat diakses dengan cepat setelah kegagalan atau pelanggaran keamanan.

8. KEPATUHAN TERHADAP STANDAR KEAMANAN (COMPLIANCE WITH SECURITY STANDARDS)

Pengembangan perangkat lunak sering kali mengikuti standar kepatuhan keamanan, seperti **GDPR** untuk data pribadi di Eropa, **HIPAA** untuk informasi kesehatan di AS, atau **PCI-DSS** untuk data pembayaran. Standar ini menetapkan pedoman ketat untuk melindungi data pengguna dan membatasi akses hanya untuk pihak yang berwenang.

9. DAFTAR REFERENSI

1. Dai, Y., Liu, Y., Zhang, J., & Tang, Y. (2020). *Data Security in Software Development: Techniques and Best Practices*. *Journal of Software Engineering and Applications*, 13(3), 75-88. doi:10.4236/jsea.2020.133006

2. **Laudon, K. C., & Laudon, J. P.** (2018). *Management Information Systems: Managing the Digital Firm* (15th ed.). Pearson Education
3. Zhang, Y., et al. (2019). "Biometric authentication methods in the modern security landscape." *Journal of Information Security*, 10(2), 57-68. doi:10.4236/jis.2019.102005
4. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of Applied Cryptography*. CRC Press.
5. Sandhu, R., et al. (1996). "Role-Based Access Control Models." *IEEE Computer*, 29(2), 38-47. doi:10.1109/2.485845.
6. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
7. Scarfone, K., & Mell, P. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)." *National Institute of Standards and Technology (NIST)*, Special Publication 800-94
8. Bishop, M. (2003). *Computer Security: Art and Science*. Addison-Wesley.
9. OWASP Foundation. (2021). *OWASP Top Ten: The Ten Most Critical Web Application Security Risks*.
10. Gartner, Inc. (2020). "Best Practices for Data Backup and Recovery in the Cloud Era."
11. European Union. (2016). *General Data Protection Regulation (GDPR)*. Official Journal of the European Union.
12. Health and Human Services (HHS). (2003). *Health Insurance Portability and Accountability Act (HIPAA) Security Rule*

10. Daftar Bacaan

1. Sama seperti pada daftar referensi

11. JADWAL PERKULIAHAN DAN TOPIK BAHASAN

Pertemuan Ke-	TOPIK BAHASAN	BACAAN
1	a. Kontrak Perkuliahan, Perkenalan dan Penjelasan b. Pengenalan Rekayasa Perangkat Lunak	Kontrak Perkuliahan
2	a. Karakteristik perangkat lunak b. Komponen perangkat lunak c. Model perangkat lunak d. Fungsi dan peran dari software engineer	1-6

3	a. Definisi SDLC b. Jenis-jenis SDLC	Idem
4	a. Observasi dan estimasi dalam perencanaan proyek b. Tujuan perencanaan proyek c. Manajemen proyek perangkat lunak yang efektif	Idem
5	a. Proses analisis kebutuhan b. Metode analisis kebutuhan c. Spesifikasi dan validasi kebutuhan	Idem
6	a. Perangkat bantu proses analisis kebutuhan b. Konsep dasar, Konteks, Proses, dan Prinsip Perancangan Perangkat Lunak; c. Isu mendasar dalam perancangan perangkat lunak	Idem
7	a. Alat bantu perancangan (DFD dan UML) b. Macam-macam diagram yang terdapat pada UML (Class Diagram, Use Case Diagram, Activity Diagram, Sequence Diagram)	Idem
8	UTS	
9	a. Konsep dalam User Interface b. Prinsip Desain Antarmuka (user experience, user guidance, user diversity)	Idem
10	a. Perencanaan dalam pengujian b. Proses testing: (black box testing, white box testing) c. Integration testing dan user testing d. Faults, Error dan Failures	Idem
11	Review Teknik Pengujian Perangkat Lunak dari proses testing	Idem
12	Pengujian unit, Pengujian integrasi, Pengujian sistem, Pengujian Penerimaan	Idem
13	a. Quality assurance pada perangkat lunak b. Keamanan data akses	Idem
14	Definisi pemeliharaan perangkat lunak dan Konsep Pemeliharaan Perangkat lunak	Idem
15	Teknik pemeliharaan perangkat lunak (Pemeliharaan korektif, pemeliharaan adaptif, pemeliharaan perfektif, pemeliharaan preventif)	Idem
16	UAS	