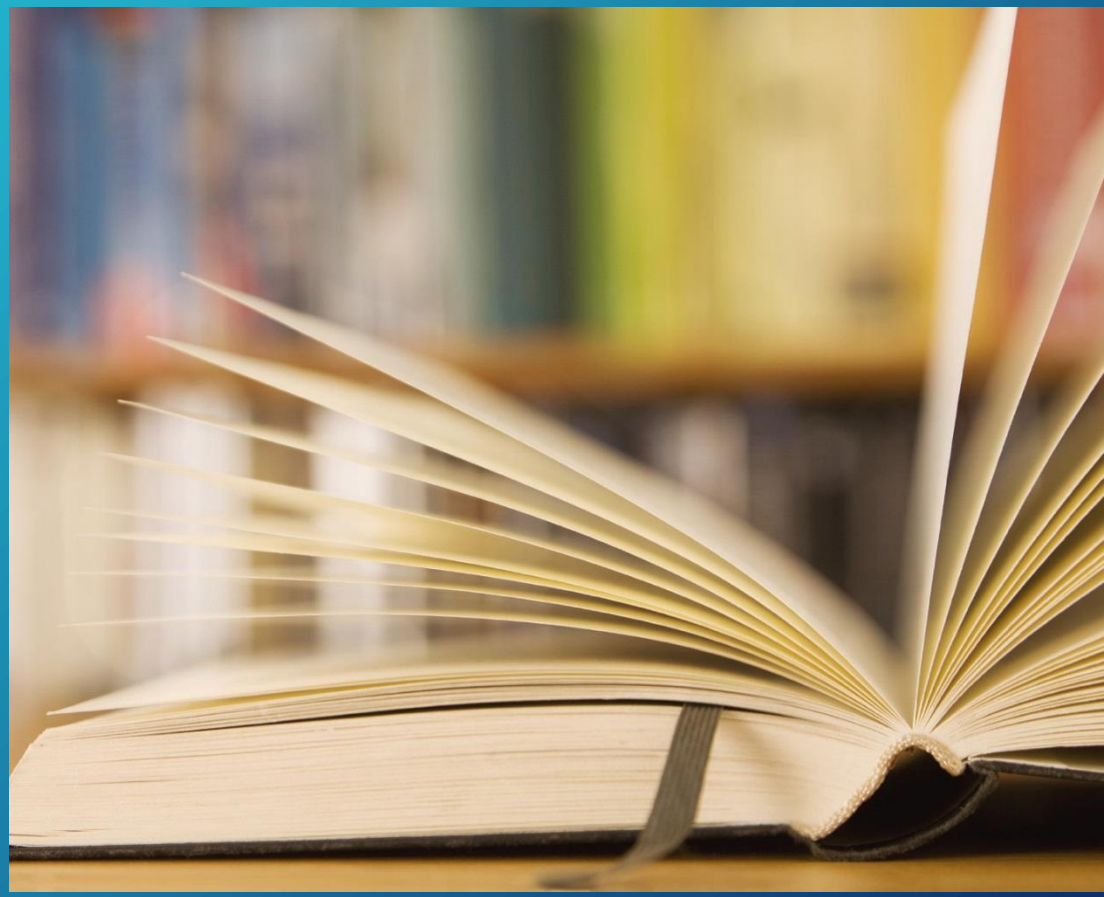
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

OTENTIKASI



Keamanan Sistem Informasi – Aditya Putra, ST., MT.

Agenda

- Access Control
- Identifikasi
- Otentikasi
- Metode Otentikasi
- Teknik Identifikasi dan Otentikasi: Password
- Teknik Identifikasi dan Otentikasi: Password Selection
- Teknik Identifikasi dan Otentikasi: Password Security
- Teknik Identifikasi dan Otentikasi: Biometrik
- Teknik Identifikasi dan Otentikasi: Token
- SSO

Access Control

Access Control adalah salah satu tema utama dalam security. Access control berperan dalam mengatur interaksi antara subjek dan objek dimana

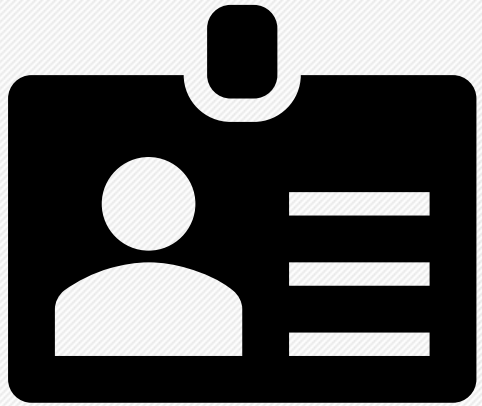
- Subjek ➔ entitas aktif yang **melakukan** akses, pencarian, menerima informasi/data dari entitas pasif/objek. Contohnya: user, program, printer, dll
- Objek ➔ entitas dimana data itu tersimpan. Contohnya: file, database, computer, program, prosess, file, printer, media penyimpanan, dll

Identifikasi

Identifikasi dan Otentikasi adalah dua contoh proses yang ada dalam mekanisme Access Control

Identifikasi adalah tindakan seorang user saat menyatakan identitasnya ke sebuah sistem

User menyatakan identitasnya dengan melakukan input username/logon ID dan password sebagai dua factor untuk mengkonfirmasi kebenaran identitasnya. Dengan inilah suatu Sistem Informasi dapat mengenali identitas user. Sistem Informasi tidak dapat mengenali manusia namun SI mengetahui bahwa akun user satu berbeda satu dengan yang lainnya.



Otentikasi

Otentikasi adalah proses verifikasi bahwa identitas yang diklaim user adalah benar dan biasanya dilakukan dengan cara matching user password saat log in.

Otentikasi mensyaratkan user untuk menyediakan factor lain untuk mengkonfirmasi identitas user.

Bentuk otentikasi paling umum adalah password yang merupakan satu di antara 3 tipe otentikasi:

- **Something you know**: Password, PIN, kombinasi kunci, nama ibu, warna favorit, dll
- **Something you have:** Smart Card, Device Token, Lokasi/Koordinat, dll
- **Something you are:** Fingerprint, Voice print, Retina, Iris, Bentuk Wajah, Telapak Tangan, Pola Berjalan, dll

Pada implementasi *two-factor authentication (TFA)*, otentikasi yang digunakan wajib menggunakan 2 metode yang berbeda kategori

Teknik Identifikasi dan Otentikasi

PASSWORD

Password adalah otentikasi yang paling umum dan sekaligus paling lemah karena beberapa alasan:

- User lebih menyukai password yang mudah diingat namun di sisi lain menjadikannya lebih mudah ditebak/dicrack
- Random password kuat namun justru membuat orang menuliskannya sehingga mudah dibaca orang lain
- Mudah ditulis, di-share, dan dilupakan
- Ditransmisikan dalam bentuk plaintext atau dengan protocol enkripsi yang mudah
- Mudah ditebak menggunakan brute force attack

Teknik Identifikasi dan Otentikasi

PASSWORD SELECTION

Password bisa menjadi efektif jika dipilih dan diatur dengan baik. Ada 2 tipe password:

- Dynamic ➔ berubah setiap interval waktu

  Contohnya adalah one-time password (OTP). OTP adalah tipe password yang berubah setiap periode waktu atau berubah setiap kali digunakan. OTP sering kita temukan saat pertama kali kita install aplikasi WA/Telegram. Server WA/Telegram akan mengirimkan kode OTP melalui SMS yang berlaku selama jangka waktu tertentu saja.

- Static ➔ selalu sama

  Sebaliknya Static Password cenderung tetap sebelum diganti oleh user secara manual. Semakin lama password tidak diubah, semakin mungkin password tersebut akan di-crack

Teknik Identifikasi dan Otentikasi

PASSWORD SECURITY

Hacker memiliki beberapa metode untuk mendapatkan sebuah password seperti Analisa trafik network (sniffing), brute force attack, dictionary attack, dan social engineering

Ada beberapa cara untuk meningkatkan keamanan password.

- Gunakan enkripsi yang kuat untuk password storage
- Jangan pernah kirimkan password dalam bentuk plaintext atau enkripsi yang lemah
- Disable user account yang tidak aktif untuk sementara. Dan hapus user account sudah tidak dipakai lagi
- Latih user tentang perlunya mengatur keamanan dan menggunakan password yang kuat. Ajarkan untuk tidak mencatat dan share user/pass

Teknik Identifikasi dan Otentikasi

BIOMETRIK

Biometrik adalah Teknik otentikasi berdasarkan karakteristik tingkah laku dan fisiologis yang unik pada setiap subjek. Contohnya adalah fingerprint, face scan, iris, retina, telapak tangan, pola denyut jantung, suara, dll

Tantangan Otentikasi Biometrik adalah bahwa akurasi dari sensornya. Faktor-factor seperti aliran darah pada retina dan nada pada suara seseorang cenderung sama dan mengacaukan akurasi. Hal ini bisa menimbulkan False Negative (FN) dan False Positive (FP). Lihat diagram di samping untuk mengetahui FN, FP, TP, dan TN

An Aesop's Fable: The Boy Who Cried Wolf (*compressed*)

A shepherd boy gets bored tending the town's flock. To have some fun, he cries out, "Wolf!" even though no wolf is in sight. The villagers run to protect the flock, but then get really mad when they realize the boy was playing a joke on them.

[Iterate previous paragraph *N* times.]

One night, the shepherd boy sees a real wolf approaching the flock and calls out, "Wolf!" The villagers refuse to be fooled again and stay in their houses. The hungry wolf turns the flock into lamb chops. The town goes hungry. Panic ensues.

Let's make the following definitions:

- "Wolf" is a **positive class**.
- "No wolf" is a **negative class**.

We can summarize our "wolf-prediction" model using a 2x2 confusion matrix that depicts all four possible outcomes:

True Positive (TP): • Reality: A wolf threatened. • Shepherd said: "Wolf." • Outcome: Shepherd is a hero.	**False Positive (FP):** • Reality: No wolf threatened. • Shepherd said: "Wolf." • Outcome: Villagers are angry at shepherd for waking them up.
False Negative (FN): • Reality: A wolf threatened. • Shepherd said: "No wolf." • Outcome: The wolf ate all the sheep.	**True Negative (TN):** • Reality: No wolf threatened. • Shepherd said: "No wolf." • Outcome: Everyone is fine.

Teknik Identifikasi dan Otentikasi

TOKEN

Token adalah device pembuat password yang harus selalu dibawa subjek Ketika ingin digunakan. Contohnya adalah ATM dan Token Internet Banking. Ada 4 jenis Token yaitu:

- Static Token: token sederhana berbentuk fisik namun masih membutuhkan otentikasi lain seperti password/PIN. Contoh: Smart Card, Swipe Card
- Synchronous Token: token ini men-generate (membuat) password setiap periode waktu tertentu. Token ini memerlukan sinkronisasi antara waktu pada server dan waktu pada device otentikasi. Contoh: Google Authenticator

Teknik Identifikasi dan Otentikasi

TOKEN

- Asynchronous Token: Token ini men-generate password saat subjek/user meng-klik tombol pada device token dan pada server otentikasi. Contoh: Token internet banking
- Challenge response Token: token ini mengenerate password berdasarkan instruksi dari server/ system otentikasi. Contoh: Captcha

Single Sign On

Single Sign On adalah mekanisme yang memungkinkan subjek hanya melakukan satu kali otentikasi saja

Single Sign On memudahkan user dan meningkatkan user experience, namun disini juga menjadi kelemahannya. Ketika user password berhasil diretas, maka seluruh akses ke resource sistem tersebut dapat diakses.

Contoh pengguna dari Single Sign On adalah Google. Ketika kita sudah login GMAIL, maka kita bisa akses YOUTUBE, G-DRIVE, G-FORM, dan seluruh aplikasi Google lainnya