BAB 12

PRIVACY & CONFIDENTIALITY

PRIVASI

- Secara bahasa Privasi dapat di artikan hak untuk dibiarkan atau hak untuk mengontrol publikasi yang tidak diinginkan tentang urusan personal seseorang.

- Secara umum, pengertian privasi adalah Kerahasiaan pribadi (privacy) adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka.

Ada 3 faktor yang mempengaruhi Privasi

- Faktor Personal
- Faktor Situasional
- Faktor Budaya.

Faktor Personal

Perbedaan dalam latar belakang pribadi akan berhubungan dengan kebutuhan akan privasi.

Contoh : anak-anak yang tumbuh dalam suasana rumah yang sesak akan lebih memilih keadaan yang anonim dan reserve saat ia dewasa. Sedangkan orang menghabiskan sebagian besar waktunya di kota akan lebih memilih keadaan anonim dan intimacy.

Faktor Situasional

Misal dalam dunia kerja kepuasaan terhadap kebutuhan akan privasi sangat berhubungan dengan seberapa besar lingkungan mengijinkan orang-orang di dalamnya untuk menyendiri.

Faktor Budaya

Misal di dalam Budaya, pada tiap–tiap budaya tidak ditemukan adanya perbedaan dalam banyaknya privasi yang diinginkan, tetapi sangat berbeda dalam cara bagaimana mereka mendapatkan privasi.

Nilai-nilai dalam Privasi

- Privasi memberikan kemampuan untuk menjaga informasi pribadi yang bersifat rahasia sebagai dasar pembentukan otonomi individu.
- Privasi dapat melindungi dari cacian dan ejekan orang lain, khususnya dalam masyarakat dimana toleransi masih rendah, dimana gaya hidup dan tingkah laku aneh tidak diperkenankan.
- Privasi merupakan mekanisme untuk mengontrol reputasi seseorang. Semakin banyak orang tahu tentang diri kita semakin berkurang kekuatan kita untuk menentukan nasib kita sendiri
- Privasi merupakan perangkat bagi berlangsungnya interaksi social.
- Privasi merupakan benteng dari kekuasaan pemerintah. Sebagaimana slogan yang berbunyi ″pengetahuan adalah kekuatan″, maka privasi menjaga agar kekuasaan tidak disalahgunakan. Pada satu sisi pemerintah memiliki privasi berupa rahasia negara yang tidak boleh dibuka dalam kondisi tertentu, pada sisi lain masyarakat juga memiliki privasi sehingga penguasa tidak berlaku semena–mena

Problematika Privasi Dalam Media

Sebagian besar media pers nasional, tidak terkecuali media arus utama (mainstream) yang bergengsi, melanggar privasi dalam penyajian beritanya.

Media pers semata mencari sensasional dan tidak disadarinya telah merugikan publik.

Permasalahan ini dinilai bentuk pelanggaran kode etik jurnalistik wartawan Indonesia yang baru, menurut wartawan menempuh cara yang profesional termasuk menghormati hak privasi atau masalah kehidupan pribadi seseorang.

Contoh kasus : Sering kali kita mendengar / melihat berita berita gosip dari para selebritis tentang kehidupan pribadi, yang seharusnya tidak layak untuk diberitakan, namun karena media ingin mendapatkan rating atau demi penonton, maka hal tersebut di siarkan.

CONFIDENTIALITY

- Maksudnya secara singkat sama dengan arti katanya yaitu kerahasian.

- Kerahasian dalam hal ini adalah informasi yang kita miliki pada sistem/database kita, adalah hal yang rahasia dan pengguna atau orang yang tidak berkepentingan tidak dapat melihat/mengaksesnya.

- **Kerahasiaan** - berkaitan dengan pengobatan informasi bahwa seseorang telah diungkapkan dalam hubungan kepercayaan dan dengan harapan bahwa hal itu tidak akan diungkapkan kepada orang lain tanpa izin dengan cara yang tidak sesuai dengan pemahaman tentang pengungkapan aslinya.

- Privacy terkait dengan kerahasiaan data-data pribadi, seperti nama lengkap, alamat, tempat tanggal lahir, status pernikahan, nama istri/suami, nama anak, tempat pekerjaan, nama ibu (mother's maiden name), status kesehatan (pernah mengidap penyakit apa saja), dan seterusnya.
- Banyak yang tidak menganggap penting untuk merahasiakan hal ini, padahal itu sangat penting untuk dirahasiakan.
- Data-data pribadi yang diberikan kepada pihak lain, misalnya ke bank, disebutkan confidential . Pihak kedua ini tidak boleh menggunakan data-data tersebut untuk keperluan lain. Mereka tidak boleh menjual data-data tersebut.
- Confidentiality juga terkait dengan data-data lain yang bukan data-data pribadi. Password (kata sandi untuk masuk ke sistem) dan PIN (kombinasi angka untuk mengakses account di bank melalui mesin ATM) merupakan contoh data yang harus dirahasiakan dan bersifat confidential.

Perbedaan antara Privacy dengan Cofidentiality :

Privacy lebih ke arah data-data yang sifatnya privat,

Confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pedaftaran sebuah service) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Ancaman yang muncul dari pihak yang tidak berkepentingan terhadap aspek *confidentialit y* antara lain:

- *password strength* (lemahnya *password* yang digunakan, sehingga mudah ditebak ataupun di–*bruteforce*)
- *malware* (masuknya virus yang dapat membuat *backdoor* ke sistem ataupun mengumpulkan informasi *pengguna*)
- *social engineering* (lemahnya *security awareness* pengguna dimana mudah sekali untuk 'dibohongi' oleh *attacker,* yang biasanya adalah orang yang sudah dikenalnya)

Cara yang umum digunakan untuk menjamin tercapainya aspek *confidentiality* adalah dengan menerapkan enkripsi.

KRIPTOGRAFI, ENKRIPSI & DEKRIPSI

KRIPTOGRAFI

- **Kriptografi,** secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita.
- Ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data
- Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Tujuan Kriptografi

- **Kerahasiaan,** adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
- **Integritas data,** adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalamdata yang sebenarnya.

Tujuan Kriptografi

- **Autentikasi,** adalah berhubungan dengan identifikasi / pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- **Non-repudiasi,** atau nir penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman / terciptanya suatu informasi oleh yang mengirimkan / membuat.

Komponen Kriptografi

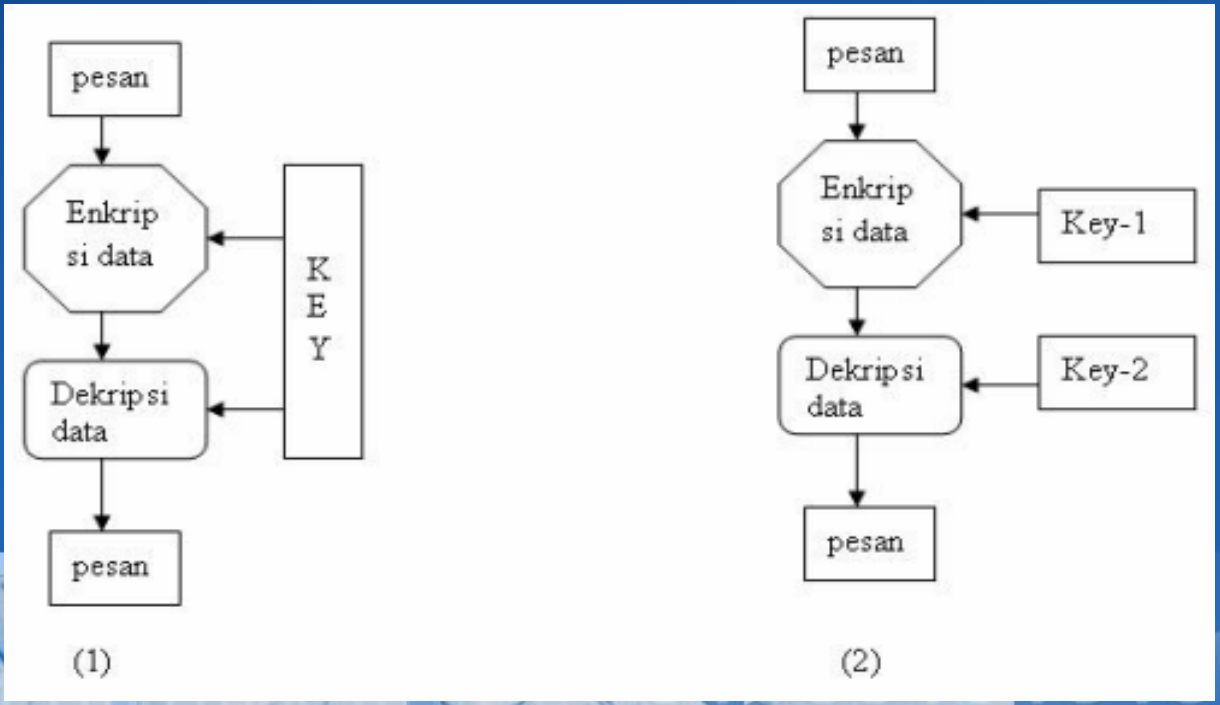
- **Plaintext,** yaitu pesan yang dapat dibaca
- **Ciphertext,** yaitu pesan acak yang tidka dapat dibaca
- **Key,** yaitu kunci untuk melakukan teknik kriptografi
- **Algorithm**, yaitu metode untuk melakukan enkrispi dan dekripsi

ENKRIPSI

- **Enkripsi** adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca).
- Enkripsi dapat diartikan sebagai kode atau chiper. Sebuah sistem pengkodean yang menggunakan suatu table atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau merupakan bagian dari informasi yang dikirim.

Teknik kriptografi data untuk enkripsi ada dua macam yaitu:

- **Kriptografi simetrik,** Dengan model kriptografi ini, data di enkripsi dan didekripsi dengan kunci rahasia yang sama.
- **Kriptografi asimetrik,** Dengan model kriptografi ini, data dienkripsi dan didekripsi dengan kunci rahasia yang berbeda. pasangan kunci untuk enkripsi dan dekripsi dikenal dengan private key dan public key.



DEKRIPSI

Dekripsi merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah cipher text menjadi plain text dengan menggunakan algortima ‘pembalik’ dan key yang sama.

TANDA TANGAN & SERTIFIKAT DIGITAL

Tujuan Penandatanganan

- **Bukti** : Sebuah tanda tangan mengotentikasikan suatu dokumen dengan mengidentifikasikan penandatangan dengan dokumen yang ditandatangani.
- **Formalitas** : Penandatanganan suatu dokumen ‘memaksa’ pihak yang menandatangani untuk mengakui pentingnya **dokumen tersebut.**
- **Persetujuan** : Dalam beberapa kondisi yang disebutkan dalam hukum, sebuah tanda tangan menyatakan persetujuan pihak yang menandatangani terhadap isi dari dokumen yang ditandatangani.
- **Efisiens** : Sebuah tanda tangan pada dokumen tertulis sering menyatakan klarifikasi pada suatu transaksi dan menghindari akibat-akibat yang tersirat di luar apa yang telah dituliskan.

Atribut dalam Penandatanganan

- **Otentikasi Penanda tangan** : Sebuah tanda tangan seharusnya dapat mengindentifikasikan siapa yang menandatangani dokumen tersebut dan susah untuk ditiru orang lain.
- **Otentikasi Dokumen** : Sebuah tanda tangan seharusnya mengidentifikasikan apa yang ditandatangani, membuatnya tidak mungkin dipalsukan ataupun diubah (baik dokumen yang ditandatangani maupun tandatangannya) tanpa diketahui.

Penggunaan tanda tangan digital memerlukan dua proses, yaitu dari pihak penandatangan serta dari pihak penerima. Secara rinci kedua proses tersebut dapat dijelaskan sebagai berikut:

- **Pembentukan tanda tangan digital** menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat yang telah didefinisikan sebelumnya. Untuk menjamin keamanan nilai hash maka seharusnya terdapat kemungkinan yang sangat kecil bahwa tanda tangan digital yang sama dapat dihasilkan dari dua dokumen serta kunci privat yang berbeda.
- **Verifikasi tanda tangan digital** adalah proses pengecekan tanda tangan digital dengan mereferensikan ke dokumen asli dan kunci publik yang telah diberikan, dengan cara demikian dapat ditentukan apakah tanda tangan digital dibuat untuk dokumen yang sama menggunakan kunci privat yang berkorespondensi dengan kunci publik.

Kelemahan & Keunggulan TTD

Kelemahan yang masih menyertai teknologi tanda tangan digital adalah:

- **Biaya tambahan secara institusional:** Tanda tangan digital memerlukan pembentukan otoritas-otoritas yang berhak menerbitkan sertifikat serta biaya-biaya lain untuk menjaga dan mengembangkan fungsi-fungsinya.
- **Biaya langganan:** Penanda tangan memerlukan perangkat lunak aplikasi dan juga membayar untuk memperoleh sertifikasi dari otoritas yang berhak mengeluarkan sertifikat.

Sedangkan kelebihan yang paling utama dari adanya tanda tangan digital adalah **lebih terjaminnya otentikasi dari sebuah dokumen**. Tanda tangan digital sangat **sulit dipalsukan** dan berasosiasi dengan kombinasi dokumen dan kunci privat secara unik.


Thank
you!