Pengantar Teknologi Informasi & Komunikasi (PTIK)

Muslim, M.InfoTech
Juwita, M.Kom
Devi Firmansyah, S.Si
Furqan Nur, S.Si

Proposal Hibah Pengembangan dan Penyelenggaraan Pembelajaran Online Berbasis E-Learning

Materi Bahasan

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

- Definisi/Pengertian
- Prinsip-prinsip Keamanan
- Pelaku serangan & motivasinya
- Jenis-jenis serangan komputer
- Cara deteksi serangan & pencegahan dini
- Keamanan akun media sosial
- Konsep Biometrika (Fingerprint, face, retina/iris, voice, dll)
- Disaster Recovery

❖Definisi/Pengertian

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

Cybercrime ➔ kejahatan yang memanfaatkan perkembangan teknologi komputer, khususnya internet.(citation1)

Cybercrime ➔ sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet. (citation2)

❖Prinsip-prinsip Keamanan Komputer

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

1. Authentikasi (ada alat pengenal => pesan original)
2. Reability (berfungsi dengan baik dan benar)
3. Integrity (sistem terpadu, pesan tidak dimodifikasi)
4. Non-repudiasi (only 1akses/1waktu/1mesin)
5. Availability (tersedia 24jam/7hari/sebulan)
6. Authority (ada otoritas penanggungjawab)
7. Access Control (ada level akses masing-masing user)
8. Confidentiality (Memastikan kerahasiaan data ➔ user org yg berhak)
9. Privacy (Bersifat pribadi)

❖Jenis-jenis ancaman komputer

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

❖Interruption (penyusupan)

- ❖ Orang yang tidak berhak menyusup diantara 2 pihak yang sedang berbagi informasi

❖Interception (Penyadapan)

- ❖ Orang yang tidak berhak berhasil menyadap lalu lintas informasi .

❖Modifikasi

- ❖Orang yang tidak berhak merubah informasi yang sedang dikirim.

❖Fabrication (pemalsuan)

- ❖Membuat informasi palsu yang mirip sekali dari pengirim asli

Jenis2 Serangan Komputer (1)

1. ***Spoofing*** ➔ seni untuk menjelma menjadi sesuatu yang lain. Spoofing attack terdiri dari IP address dan node source atau tujuan yang asli atau yang valid diganti dengan IP address atau node source/tujuan lain.
2. ***Serangan Man-in-the-middle*** *(serangan pembajakan)* ➔ terjadi saat user perusak dapat memposisikan diantara dua titik link komunikasi, dgn jalan mengkopy atau menyusup traffic antara dua party.
3. ***Spam*** ➔ yang umum dijabarkan sebagai email yang tak diundang ini, newsgroup, atau pesan diskusi forum. Spam bisa merupakan iklan dari vendor atau bisa berisi kuda Trojan.
4. ***Sniffer*** ➔ user perusak ingin mendapatkan informasi jaringan atau traffic lewat jaringan tersebut, denganprogram penangkap paket yang bisa menduplikasikan isi paket yang lewat media jaringan ke dalam file.
5. ***Crackers*** ➔ user perusak yang bermaksud menyerang suatu system atau seseorang.
6. ***Fishing*** ➔ Perusak mengintai kesalahan ketik hingga bisa masuk ke url yg salah (tapi mirip), agar bisa mencuri akun user dan passwordnya. contoh: www.klikbca.com ➔ www.kilkbca.com
7. *Defacing* ➔ *Merusak halaman muka website, menggantinya dg yg lain.*

Jenis2 Serangan Komputer (2)

8. Brute Force and Dictionary

➔ menyerang database password/login prompt yang sedang active.dg mencoba berbagai kombinasi angka, huruf, atau symbol.

➔ Dictonary: upaya menemukan password dgn mencoba berbagai kemungkinan password yang biasa dipakai user: nama, tgl lahir, dll.

9. Deniel of Services (DoS) ini adalah salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan jadi mampet, dengan cara mengirim paket data dalam jumlah yang sangat bersar terhadap suatu server dimana server tersebut tidak bisa memproses semuanya. Contoh:

- **1. *Distributed Denial of Services (DDoS)*, menguasai layanan system sebagai pusat serangan**
- **2. Distributed refelective deniel of service (DRDoS) memanfaatkan layanan Internet, menyerang dengan mengirim update, sesi, dalam jumlah sangat besar kepada layanan server atau router**
- **3. *Sync*, Serangan keamanan jaringan dengan membanjiri sinyal SYN kepada system yang menggunakan protocol TCP/IP.**
- ***4. Smurf attack,* sebuah server digunakan untuk membanjiri korban dengan data sampah.**
- ***5. Ping of death,* serangan ping yang oversize menyebabkan system crash, freeze atau reboot.**
- ***6. Stream Attack* terjadi saat banyak jumlah paket yang besar dikirim menuju ke port pada system korban menggunakan sumber nomor yang random.**

❖Pelaku serangan & motivasinya

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

8 WNA penipuan via FB

48 WNA mafia Judi Online

1. Hacker ➔ uji kepandaian
2. Cracker ➔ merusak
3. Terorist ➔ mencari dana/pengikut
4. Pelajar/Mhs ➔ coba-coba (kepo)
5. Expert ➔ tes system
6. IRT ➔ mencari biaya tambahan
7. Cyber cop ➔ mencari penjahat
8. Mantan (Karyawan) ➔ Dendam
9. Perusahaan saingan ➔ Curi info
10. WNA ➔ Bisnis Ilegal (baru)

❖ Cara deteksi serangan

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

❖Anomaly Detection (Penyimpangan)

➔mengidentifikasi perilaku tak lazim yang terjadi dalm Host atau Network.

❖Misuse Detection

➔Detektor melakukan analisis terhadap aktivitas sistem, mencari event atau set event yang cocok dengan pola perilaku yang dikenali sebagai serangan.

❖Network Monitoring

➔(sistem pemantau jaringan) untuk mengatahui adanya lubang keamanan, Biasanya dipakai (SNMP)

❖Intrusion Detection System (IDS)

➔Penghambat atas semua serangan yg akan

Pencegahan Dini

Aset ➔ Perlindungan aset merupakan hal yg penting dan merupakan langkah awal dari berbagai implementasi keamanan komputer.

Analisa Resiko ➔ Identifikasi akan resiko yg mungkin terjadi, sebuah even yg potensial bisa mengakibatkan suatu sistem dirugikan.

Perlindungan ➔ Pada era jaringan, perlu dikwatirkan keamanan dari sistem komp, baik PC atau yg terkoneksi dgn jaringan

Alat ➔ Tool yg digunakan pd PC memiliki peran penting dlm hal

keamanan krn itu tool yg digunakan harus benar2 aman.

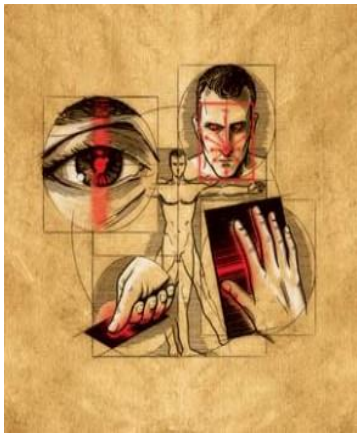
Prioritas ➔ perlindungan PC secara menyeluruh

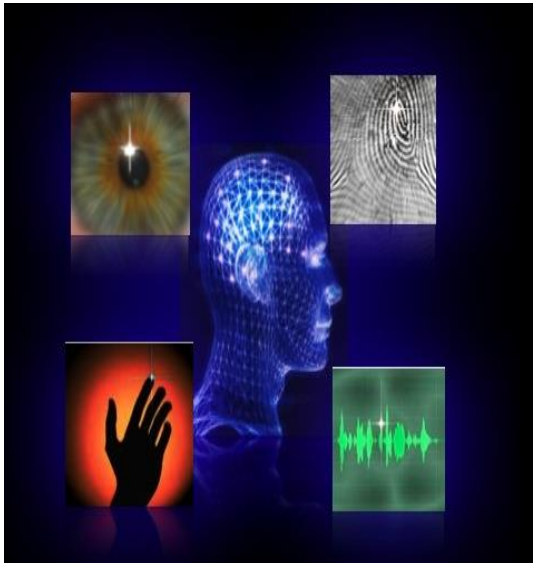
Disaster Recovery ➔ Siapkan skenario penyelamatan/pemulihan kembali sistem komputer jika terjadi bencana secara tiba-tiba *(force majeure)*

❖Konsep Biometrika

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

Biometrik ➔ suatu metode identifikasi manusia berdasarkan satu atau lebih bagian tubuh manusia atau kelakukan dari manusia, dengan menganalisa secara statistik dari karakteristiknya.





- Perangkat biometrik memiliki metode otentifikasi yang biasa digunakan yaitu dengan mengenali orang dari ciri-ciri fisiknya. Berbagai aspek manusia seperti fisiologi, kimia atau perilaku sebenarnya dapat digunakan untuk otentikasi biometrik. Metode ini diterapkan pada dunia teknologi informasi untuk proses autentifikasi atau

Fakta Sejarah

- Biometrik telah ada sekitar sejak 29.000 sebelum masehi ketika manusia gua akan menandatangani gambar mereka dengan telapak tangan.
- Pada tahun 500 sebelum masehi, transaksi bisnis orang-orang *Babilonia* sudah melakukan tanda tangan di lembaran tanah liat berupa sidik jari.
- Pertama kali katalogisasi sidik jari bermula pada 1891 saat Juan Vucetich memulai untuk mengumpulkan koleksi sidik jari para criminal di Argentina.

❖Konsep Biometrika

Oleh: Tim Hibah e-Learning FMIPA Unsyiah

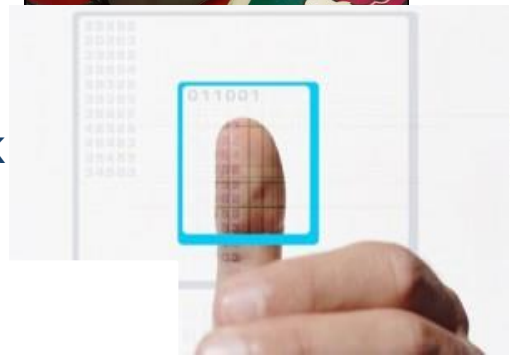
Alat tubuh yang sering dipakai sebagai biometrika:

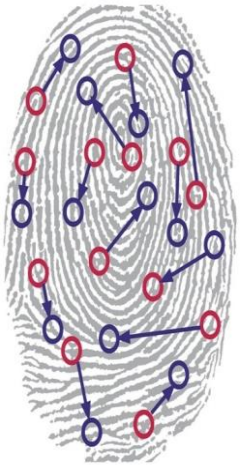
- ❖ Sidik jari (finger print)
- ❖ Muka *(face)*
- ❖ Selaput pelangi (*iris*)
- ❖ Suara (*voice*)
- ❖ Geometri tangan (*hand geometry*)
- ❖ Tanda tangan (*signature)*.

Sidik Jari

Biometrik sidik jari ➔ sistem autentikasi biometrik yang paling banyak digunakan,
➔ memiliki akurasi tinggi dan mudah diterapkan.

Sidik jari setiap manusia punya kode khusus,
- ❖ berupa garis-garis khas *macro* dan *minutae*
- ❖ Hasil pencitraan berupa data digital khas (statistik karakter guratan jari, bukan gambar jari).



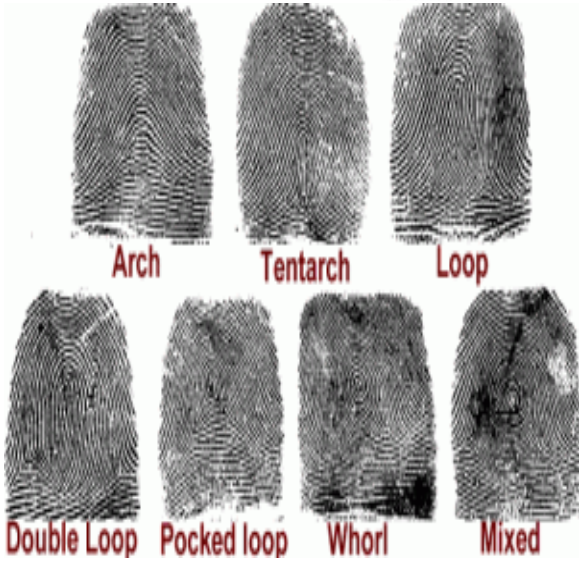


Kelebihan:

- ❖ Tidak akan menggangu, faktor error kecil dan tepat ukur.
- ❖ Penggambaran array kecil & lebih murah.

Kekurangan:

- ❖ Jika jari mengalami luka potong atau terbakar, maka akan mempengaruhi kinerja alat ini.
- ❖ Sidik jari pekerja di industri kimia



Geometri Telapak Tangan

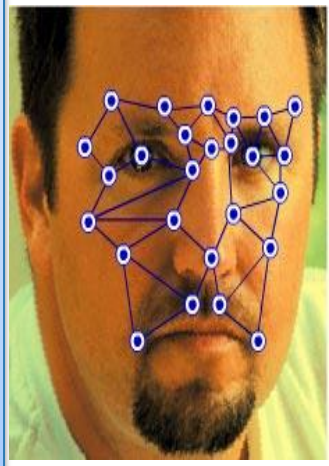
- Sistem ini bekerja atas dasar prinsip keunikan pembuluh darah telapak tangan tiap-tiap individu, bahkan kembar siam sekalipun.
- Sistem memiliki sensor yang mampu mengenali pola telapak tangan seseorang selama *hemoglobin deoxidized* atau sel darah merah dengan aktif mengaliri pembuluh darah. Dengan kata lain, hanya telapak tangan orang yang masih hidup yang dapat dideteksi.
- Salah satu vendor yang sudah memproduksi perangkat ini adalah *PT Fujitsu Systems*. PT Fujitsu Systems Indonesia meluncurkan perangkat otentifikasi pembaca tapak tangan tanpa sentuh.
- *Palm vein* ➔ merupakan teknologi keamanan biometrik yang bisa mengidentifikasi

Guratan pada Raut Wajah

- Identifikasi karakteristik bentuk wajah ➔ menggunakan alat scan panas sinyal infra merah.
- Enam bagian titik sering digunakan (titik-titik segitiga tulang muka).

  a. Bagian titik ini terdiri atas ➔ **mata, mulut dan alis mata.**

  Akan tetapi jarak antar bagian mata tidaklah cukup diperoleh secara langsung dari bagian titik muka, untuk itu diperlukan suatu bentuk metode pada bagian daerah mata.



  b. Bagian lain ➔ mulut, ini secara global tidaklah cukup untuk menguraikan bentuk mulut. Untuk mendapatkan bagian ini, bagian wajah dinormalisir berdasarkan tepian dari pemetaan.

- Sistem pengenalan wajah sebagai kunci (*password*) menggunakan ekspresi seseorang yang tanpa dibuat-buat (*dramatic*) ➔ *relaxed face*.
- Para psikolog menggolongkan ekspresi wajah ini, secara universal ke dalam 6 (enam) bentuk ➔ *happines*, *sadness*, *disgust*, *anger*, *surprise* dan *fear*.
- Dari enam ekspresi wajah ini, dapat dibangun suatu sistem

Retina Mata (Iris & Kornea)

- Retina mata➔terlindung dan terproteksi dari lingkungan luar.
- Mata memiliki sifat fisiologi, ukuran & ketajaman reaksi terhadap cahaya yang berbeda-beda.
- Bereaksi thdp cahaya dan gerakan/getaran alami untuk mencegah perubahan pada gambar /subjek lain yang mengarah padanya.
- Retina mata ➔ di dalamnya terdapat iris atau selaput pelangi.
- Letak selaput pelangi ini berada antara kornea dan lensa mata.
- Selaput pelangi terlihat dari luar mata, punya pola unik, konsisten dan stabil

Retina Mata (Iris & Kornea)

- *Iris recognition* ➔ menggunakan selaput pelangi mata yang dikodekan secara digital dan kemudian dijadikan kunci. Proses otentifikasinya membutuhkan dua tahap yakni tahap identifikasi dan tahap verifikasi. Proses ini dapat dilakukan secara *one-to-many* (1:m) atau *one-to-one* (1:1).
- Proses *one-to-many* akan melibatkan satu *database* yang berisi *user id* dan *iris template* pada masing-masing id. Proses *capture* akan dilanjutkan dengan *searching database* untuk mencari *iris template* yang cocok. Sedangkan proses *one-to-one* akan lebih pada membandingkan dua iris, yaitu hasil scan dan iris template yang sudah disimpan.
- Dari kedua proses ini sudah tentu proses *one-to-one* lebih disukai karena prosesnya lebih cepat. Ini disebabkan oleh pembandingan yang dilakukan dalam skala terbatas.

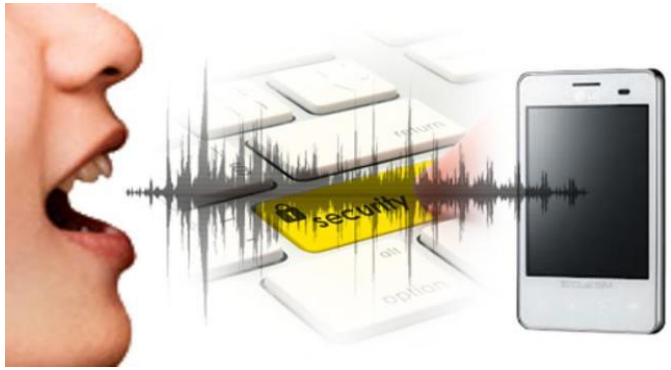
Retina Mata (Iris & Kornea)

- **Kelebihan:**
  - **Merupakan biometrik identifikasi yang sangat akurat.**
  - **Pola retina yang unik dan sangat sulit ditiru.**
  - **Sangat sedikit *False Acceptance Rate (Diterima sistem padahal salah user)* dan *False Rejection Rate (ditolak sistem, padahal user orang yg benar)*.**

- **Kekurangan:**
  - **Untuk orang yang terkena diabetes, mata bisa terpengaruh sehingga ada perbedaan.**
  - **Membutuhkan kontak dekat dengan mata pengguna, sehingga agak mengganggu.**
  - **Mengharuskan pengguna untuk melepas kacamata/lensa sebelum melakukan pemindaian.**

Suara (Frekwensi & Intonasi)

❖ Suara manusia ➔ khas dan unik,
❖ dapat dibedakan antara satu manusia dengan manusia lainnya ➔ bedaan frekuensi, intonasi suara karena jenis suara tidak ada yang sama persis.
❖ Aspek yang dapat menjadi perbandingan adalah dasar suara yang keluar dari hidung, gerakan jakun, irama, tingkat suara, frekuensi dan durasi.



❖ Kelebihan:
- Non intrusif. Penerimaan sosial tinggi.
- Waktu Verifikasinya sekitar lima detik.
- Teknologi termasuk murah.

❖ Kekurangan:
- Mudah direkam dan digunakan untuk PC atau jaringan yang tidak sah.
- Akurasinya rendah.
- Karena faktor usia, suara seseorang bisa berbeda.
- Penyakit seperti pilek / infeksi tenggorokan ➔ dapat mengubah suara seseorang, sehingga proses identifikasi menjadi sulit atau bahkan tidak memungkinkan, maka metode verifikasi ini tidak bisa dilaksanakan setiap saat.

Tanda Tangan

- Tanda tangan ➔ dg papan dan pena khusus.
- Pemakai menulis tanda tangan, dengan cara penciriannya,
- Bukan membandingkan bentuk tanda tangan, tetapi membandingkan gerakan (arah) dan tekanan pada pena saat menulis.
- Seseorang dapat meniru tanda tangan [illegible] persis cara (gerakan dinamis dan ira[illegible] pembuatan tanda tangan.

- Kelebihan:
  - Non intrusif,
  - Sedikit waktu verifikasi (sekitar li[illegible]
  - Teknologinya murah.
- Kekurangan:
  - Verifikasi tanda tangan dirancang untuk memverifikasi subyek berdasarkan ciri-ciri tanda tangan masing-masing yang unik. Akibatnya, seseorang yang

Thank You !