KEAMANAN INFORMASI
10. BIOMETRIC AUTHENTICATION

Doni Abdul Fatah
github.com/doniaft
Universitas Trunojoyo Madura

Pokok Bahasan

01. Pengantar Keamanan Informasi

02. Pemodelan Serangan (Attack Tree)

03. Sistem Keamanan Informasi dan Internet

04. Autentikasi

05. Kontrol Akses

06. Firewall dan Intrusion Detection System

07. Network Attack

08. Kriptografi

09. Kriptografi Asimetrik

10. Biometric Authentication

11. Public Key Infrastructure

12. Protokol Keamanan

13. Malware & Computer Forensics

14. UAS

01. Keamanan Informasi

1) Public Key Infrastructure
2) Biometric Authentication
3) Contact
4) Referensi

10. Biometric Authentication

Biometric

- “You are your key” Schneier
- Contoh :
  - Sidik Jari
  - Tandatangan
  - Deteksi Retina
  - Deteksi Wajah
  - Deteksi Suara
  - Deteksi cara berjalan
  - Deteksi bau (odor) / digital doggie
  - Dan lain2

Karakteristik Ideal

- Universal → dapat diaplikasikan ke semua orang
  - Orang cacat mungkin tidak mempunyai sidik jari
- Distinguishing → dapat membedakan dg pasti
  - Adakah 2 orang yang mempunyai sidikjari yang sama ?
- Permanent → tidak berubah selama hidup seseorang
  - Wajah seseorang berubah sepanjang usia
- Collectable → mudah mendapatkan data
  - Belum tentu semua orang kooperatif
- Aman, user friendly, dll

Mode Biometrik

- Identifikasi
  - one-to-many
  - Contoh: Database sidik jari yang dipunyai polisi
- Autentikasi
  - one-to-one
  - Contoh: Penggunaan sidik jari untuk login
- Identifikasi lebih sulit dibandingkan Autentikasi

Tahapan

- Fase pengambilan data / pendaftaran
  - Data biometrik pengguna diambil dan dimasukkan database
  - Harus dilakukan secara hati-hari dan mungkin diperlukan beberapa kali pengambilan data
  - Harus ada prosedur yang aman untuk memvalidasi identitas pengguna dengan biometrik nya (supaya tidak ada orang yang memalsukan data orang lain dengan data biometrik dirinya)
- Fase deteksi / autentikasi
  - Deteksi data biometrik dan dibandingkan dengan database
  - Harus cepat dan nyaman
  - Akurasi tinggi

Kesalahan Biometrik

- Fraud rate versus insult rate
  - False Negative / Fraud (A dikenal sebagai B)
  - False Positive / Insult (A tidak dikenal sebagai A)
- Digunakan secara tepat
  - 99% voiceprint match → low fraud, high insult
  - 30% voiceprint match → high fraud, low insult
- Equal error rate: dimana fraud == insult
  - Harus diperhitungkan secara tepat
  - Kenyamanan vs Keamanan

Sidik Jari

- Feature : loops, whorls, dan arches
- Menggunakan feature extraction

Loop (double)

Whorl

Arch

Sidik Jari: Pendaftaran

- Tangkap gambar sidik jari
- Diperjelas
- Ekstraksi fitur

Tahap Pengenalan

- Point / fitur yang sudah diekstraksi dibandingkan dengan yang ada di database
- Apakah sama ?

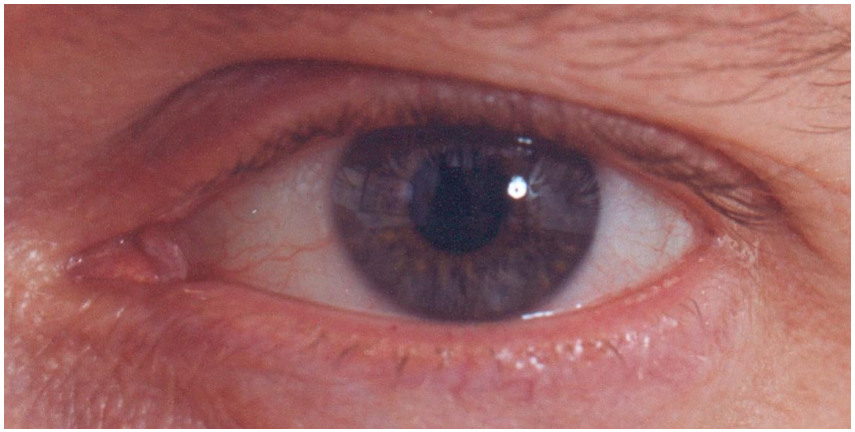
Hand Geometry

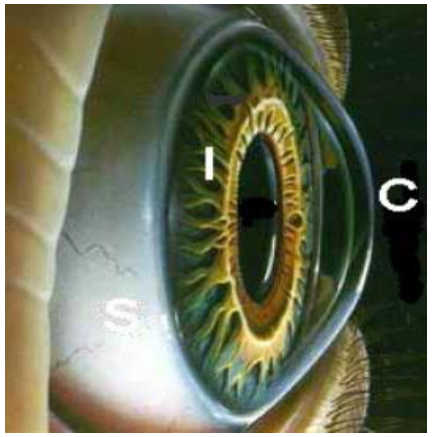
- Mengukur bentuk tangan
  - Lebar telapak, lebar jari
  - Panjang jari, dll
- Tangan manusia tidak unik
- Hanya bisa digunakan untuk aplikasi tertentu saja
- Dapat digunakan untuk autentikasi tetapi tidak untuk identifikasi

Hand Geometry

- **Keuntungan :**
  - Cepat dalam proses pendataan dan proses pendeteksian
  - Tangan kiri dan kanan (hampir) mempunyai fitur ukuran yang sama
- **Kelemahan :**
  - Tidak dapat digunakan pada user yang terlalu muda atau terlalu tua
  - Error rate cukup tinggi

Pola Iris





- Mempunyai pola yang unik untuk setiap orang
- Sedikit sekali dipengaruhi oleh faktor genetis
- Orang kembar mempunyai pola iris yang berbeda
- Pola relatif tidak berubah sepanjang hidup

Menghitung Kedekatan Iris

Menggunakan Hamming Distance

- d(x,y) = jumlah bit yg tidak match / jumlah bit yang dibandingkan
  - d(0010,0101) = 3/4
  - d(101111,101001) = 1/3
- Hitung d(x,y) untuk kode iris 2048-bit
  - Sama persis → d(x,y) = 0
  - Untuk iris yang sama maka d = 0.08
  - Nilai threshold untuk diterima adalah d < 0.32

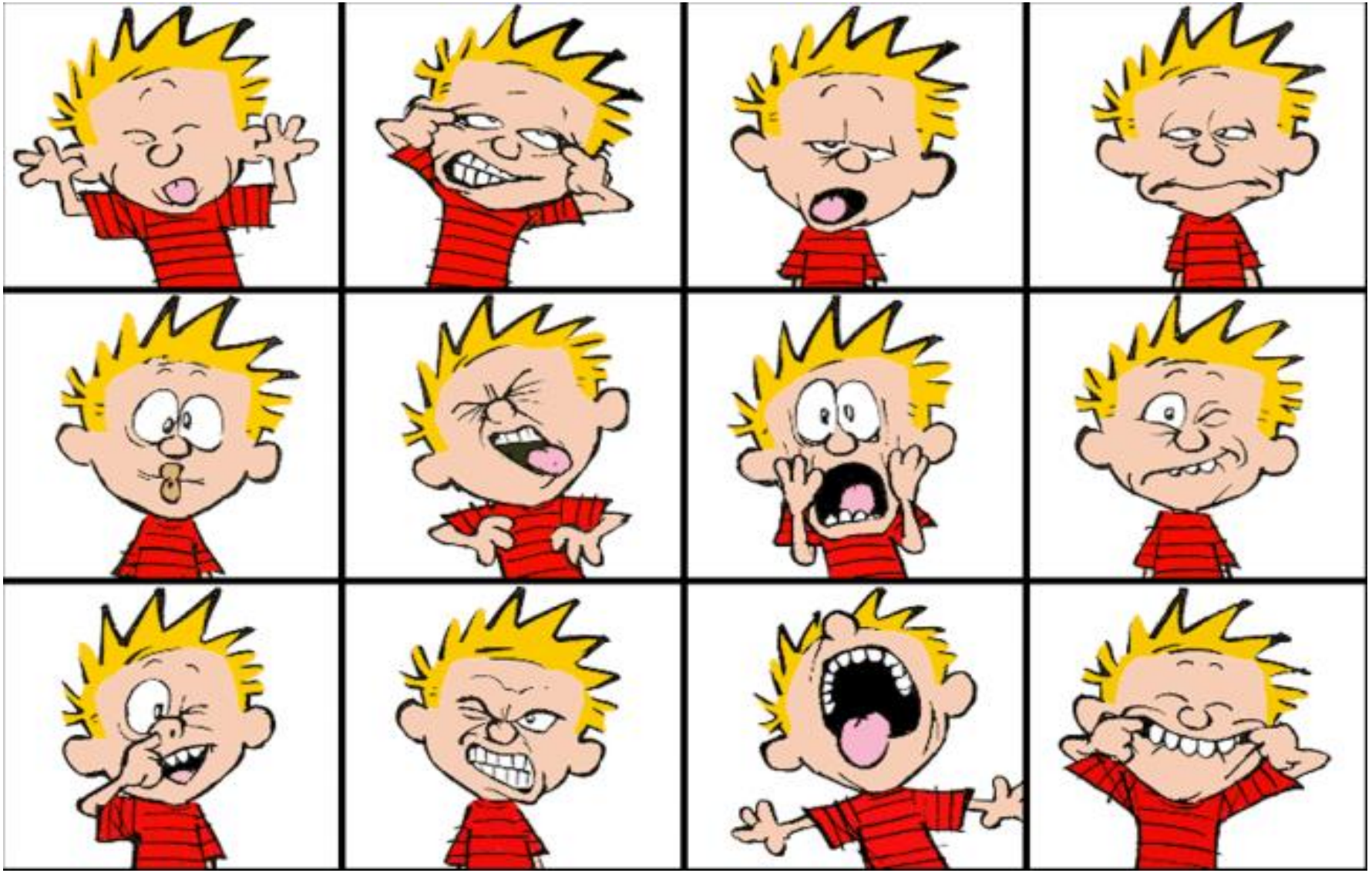
Serangan pd Iris Scan

- Penyerang menggunakan photo seseorang (dalam film-film action menggunakan bola mata subyek)
- Sistem pemindai harus bisa membedakan antara mata palsu / photo dengan mata aseli / hidup
- Bisa menggunakan pemindai dengan sinar infra merah, atau mendeteksi pergerakan pupil yang disoroti sinar secara acak

Pengenalan Wajah

- Membutuhkan ekspresi yang natural
- Subyek menatap lurus ke kamera
- Pencahayaan yang stabil
- Algoritma untuk memproses, mengekstrak fitur, dan membandingkan antara database dengan hasil pindaian

Pengenalan Wajah



Tingkat Perbandingan

- Equal error rate (EER): fraud == insult rate
- Fingerprint biometric mempunyai EER ~ 5%
- Hand geometry → EER ~ 10-3
- Secara teori, iris scan mempunyai ERR ~ 10-6
  - Teori dan praktek berbeda :)
- Biometrik lainnya tidak lebih baik dari sidik jari
- Biometrik sangat berguna untuk autentikasi
- Penggunaan DNA memerlukan waktu yang lama dan peralatan khusus

Biometrik

- Tidak mudah memalsukan Biomterik
- Tetapi penyerang dapat melakukan :
  - Pencurian data biometrik
  - Membajak software pemindai, alat, dll
- **Biometrics tetap memiliki kelemahan**
- **Harus digabungkan dengan faktor autentikasi lainnya (multifactor authentication)**
- **Something you know, something you have, something you are**

3) Kontrak Perkuliahan

a) Tata Tertib
b) Contact
c) Referensi

Tata Tertib Perkuliahan SI4B

- Masuk sesuai jadwal 15.25 WIB, Toleransi keterlambatan adalah 20 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4C

- Masuk sesuai jadwal 09.15 WIB, Toleransi keterlambatan adalah 15 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4D

- Masuk sesuai jadwal 12.45 WIB, Toleransi keterlambatan adalah 15 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Proyek : Kelompok
dibuat 2 s.d 4 Mahasiswa

- Membuat aplikasi sederhana dengan fokus **Keamanan Informasi dalam Penggunaan** Aplikasi/berInternet
- **Tahapannya :**
  - Penentuan Studi Kasus
  - Membuat aplikasi Login Spoofing Attack
  - Dalam aplikasi Login Spoofing Attack untuk pemberian passwordnya di lakukan dengan menggunakan teknik Kriptografi (enkripsi) dengan menggunakan enkripsi asimetris
  - Untuk memecahkan enkripsi tersebut maka dilakukan deskripsi dari enkripsi tersebut.
  - Untuk Aplikasi boleh Web atau Desktop, sesuai yang dikuasai.
  - Pembuatan Laporan atau Dokumentasi.
- **Poin penilaian:** Aplikasi, Dokumentasi, Presentasi.

5) Contact

Contact

- Bahan Kuliah : github.com/doniaft
- Email : doniaft@gmail.com
- WA/Telegram :
- Komting Keamanan Informasi
  - SI4C : Yusril : 0856 5509 5641
  - SI4D : Ikrom : 0852 3027 9767
  - SI4B :
    - Rahma : : 0852 5707 1554
    - Adi : 0899 3616 728

6) Referensi

Referensi (1)

- Anderson, Ross, “Security Engineering”, First Edition, Wiley, 2001, tersedia dalam e-Book : URL: http://www.cl.cam.ac.uk/~rja14/book.html
- Menezes et.al, “Handbook of Applied Cryptography”, Fifth Edition, CRC Printing, 2001, tersedia dalam e-Book URL: http://cacr.uwaterloo.ca/hac
- Bishop, Matt, “Computer Security: Art and Science”, Addison Wesley, 2002
- Stinson, Douglas R, “Cryptography: Theory and Practice”, CRC Press, 1995
- Electronic Frontier Foundation, “Cracking DES”, O'Reilly, 1998
- Stamp, Mark, “Computer Security: Principles and Practices”, Willey, 2011
- Eric Cole, Ronald Krutz, and James W. Conley, “Network Security Bible”,
- Wiley Publishing, Inc., 2005.
- Matthew Strebe, “Network Security Foundations”, Sybex, 2004.
- Chris McNab, “Network Security Assessment”, O’reilly, 2008.
- James D. McCabe, dkk, “Network Security Know It All”,Morgan
- Kaufmann, 2008.
- Ibisa, “Keamanan Sistem Informasi”, Penerbit Andi, Yogyakara, 2011