Tabel 3.3 Fungsi dan Data Elektronik untuk Kartu Tanda Penduduk Elektronik

Fungsi	Tujuan	Kata Sandi PACE	Data	Penggunaan
ePass (wajib)	Sistem inspeksi offline resmi membaca data	BISA atau MRZ	Gambar wajah; dua gambar sidik jari (opsional); Data MRZ	Verifikasi identitas biometrik offline disediakan untuk akses pemerintah
eID (aktivasi opsional)	Aplikasi online membaca data atau mengakses fungsi yang diotorisasi	PIN eID	Keluarga dan nama yang diberikan; nama artistik dan gelar doktor: tanggal dan tempat lahir; alamat dan ID komunitas; tanggal kedaluwarsa	Identifikasi; verifikasi usia; verifikasi ID komunitas; identifikasi terbatas (nama samaran); permintaan pencabutan
	Sistem inspeksi offline membaca data dan memperbarui alamat dan ID komunitas	BISA atau MRZ		
eSign (sertifikat opsional)	Otoritas sertifikasi memasang sertifikat tanda tangan secara online	PIN eID	Kunci tanda tangan; Sertifikat X.509	Pembuatan tanda tangan elektronik
	Warga negara membuat tanda tangan elektronik dengan PIN eSign	BISA		

BISA nomor akses kartu
MRZ zona yang dapat dibaca mesin
LAJU PIN pembuatan koneksi yang diautentikasi dengan kata sandi nomor identifikasi pribadi

layanan resmi dapat mengakses dengan izin pemegang kartu. Warga memilih apakah mereka ingin fungsi ini diaktifkan.

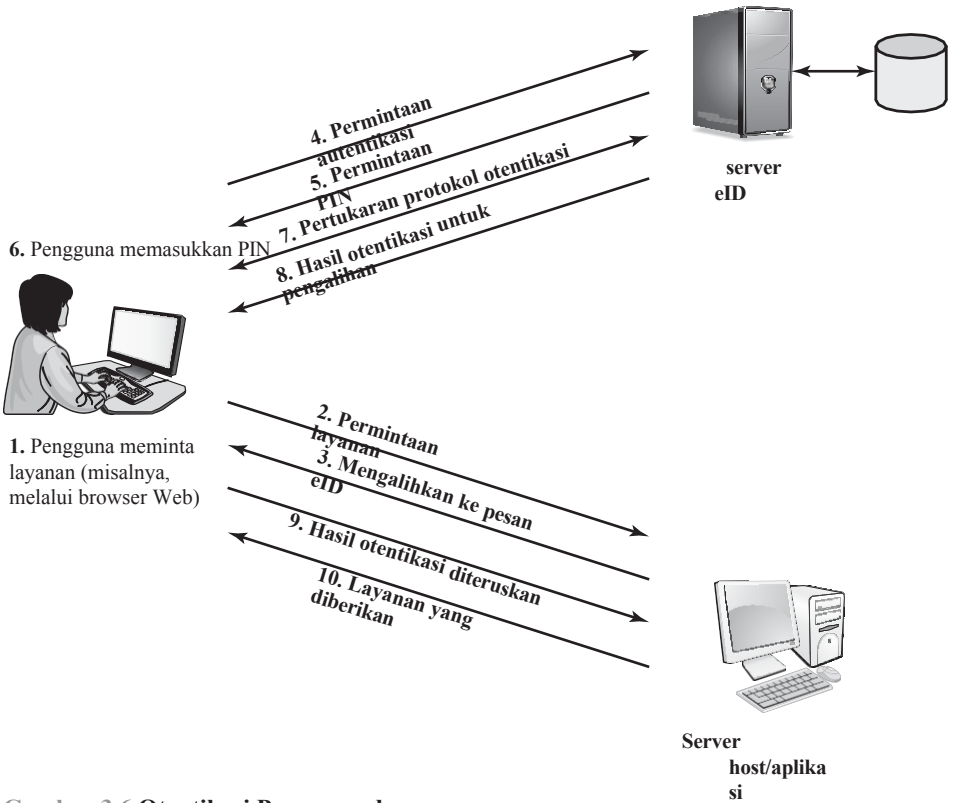
- **eSign:** Fungsi opsional ini menyimpan kunci pribadi dan sertifikat yang memverifikasi kunci tersebut; fungsi ini digunakan untuk menghasilkan tanda tangan digital. Pusat kepercayaan sektor swasta menerbitkan sertifikat tersebut.

Fungsi ePass adalah fungsi offline. Artinya, fungsi ini tidak digunakan melalui jaringan, tetapi digunakan dalam situasi di mana pemegang kartu menunjukkan kartu untuk layanan tertentu di lokasi tersebut, seperti melalui pos pemeriksaan paspor.

Fungsi eID dapat digunakan untuk layanan online dan offline. Contoh penggunaan offline adalah sistem inspeksi. Sistem pemeriksaan adalah terminal untuk

pemeriksaan penegakan hukum, misalnya, oleh polisi atau petugas pengawas perbatasan. Sistem pemeriksaan dapat membaca informasi identifikasi pemegang kartu serta informasi biometrik yang tersimpan di kartu, seperti gambar wajah dan sidik jari. Informasi biometrik dapat digunakan untuk memverifikasi bahwa individu yang memiliki kartu tersebut adalah pemegang kartu yang sebenarnya.

Otentikasi pengguna adalah contoh yang baik untuk penggunaan fungsi eID secara online. Gambar 3.6 mengilustrasikan skenario berbasis Web. Untuk memulai, pengguna eID mengunjungi situs Web dan meminta layanan yang memerlukan autentikasi. Situs Web mengirimkan kembali



Gambar 3.6 Otentikasi Pengguna dengan eID

pesan pengalihan yang meneruskan permintaan autentikasi ke server eID. Server eID meminta pengguna memasukkan nomor PIN untuk kartu eID. Setelah pengguna memasukkan PIN dengan benar, data dapat dipertukarkan antara kartu eID dan pembaca terminal dalam bentuk terenkripsi. Server kemudian melakukan pertukaran protokol otentikasi dengan mikroprosesor pada kartu eID. Jika pengguna diautentikasi, hasilnya akan dikirim kembali ke sistem pengguna untuk dialihkan ke aplikasi server Web.

Untuk skenario sebelumnya, perangkat lunak dan perangkat keras yang sesuai diperlukan pada sistem pengguna. Perangkat lunak pada sistem pengguna utama mencakup fungsi-fungsi untuk meminta dan menerima nomor PIN dan untuk pengalihan pesan. Perangkat keras yang dibutuhkan adalah pembaca kartu eID. Pembaca kartu dapat berupa pembaca kontak eksternal atau pembaca nirkontak atau pembaca nirkontak internal pada sistem pengguna.

KATA SANDI PEMBUATAN KONEKSI TERAUTENTIKASI (PACE) Kata Sandi

Pembentukan Koneksi Terotentikasi (PACE) memastikan bahwa chip RF nirkontak dalam kartu eID tidak dapat dibaca tanpa kontrol akses eksplisit. Untuk aplikasi online, akses ke kartu dibuat oleh pengguna dengan memasukkan PIN 6 digit, yang hanya boleh diketahui oleh pemegang kartu. Untuk aplikasi offline, MRZ yang tercetak di bagian belakang kartu atau nomor akses kartu enam digit (CAN) yang tercetak di bagian depan digunakan.

3.4 AUTENTIKASI BIOMETRIK

Sistem autentikasi biometrik mencoba mengautentikasi seseorang berdasarkan karakteristik fisiknya yang unik. Ini termasuk karakteristik statis, seperti sidik jari, geometri tangan, karakteristik wajah, serta pola retina dan iris mata; dan karakteristik dinamis, seperti sidik suara dan tanda tangan. Intinya, biometrik didasarkan pada pengenalan pola. Dibandingkan dengan kata sandi dan token, autentikasi biometrik secara teknis lebih kompleks dan mahal. Meskipun digunakan dalam sejumlah aplikasi tertentu, biometrik belum matang sebagai alat standar untuk autentikasi pengguna ke sistem komputer.

Karakteristik Fisik yang Digunakan dalam Aplikasi Biometrik

Sejumlah jenis karakteristik fisik yang berbeda sedang digunakan atau sedang diteliti untuk autentikasi pengguna. Yang paling umum adalah sebagai berikut:

- **Karakteristik wajah:** Karakteristik wajah adalah cara yang paling umum untuk identifikasi antar-manusia; oleh karena itu, wajar jika kita mempertimbangkannya untuk identifikasi oleh komputer. Pendekatan yang paling umum adalah menentukan karakteristik berdasarkan lokasi relatif dan bentuk fitur wajah utama, seperti mata, alis, hidung, bibir, dan bentuk dagu. Pendekatan alternatif adalah dengan menggunakan kamera inframerah untuk menghasilkan termogram wajah yang berkorelasi dengan sistem pembuluh darah di bawah kulit wajah manusia.
- **Sidik jari: Sidik** jari telah digunakan sebagai alat identifikasi selama berabad-abad, dan prosesnya telah disistematisasi dan diotomatisasi secara khusus untuk tujuan penegakan hukum. Sidik jari adalah pola tonjolan dan alur pada permukaan ujung jari. Sidik jari diyakini unik di seluruh populasi manusia. Dalam praktiknya, sistem pengenalan dan pencocokan sidik jari otomatis mengekstrak sejumlah fitur dari sidik jari untuk disimpan sebagai pengganti numerik dari pola sidik jari secara keseluruhan.
- **Geometri tangan:** Sistem geometri tangan mengidentifikasi fitur-fitur tangan, termasuk bentuk, serta panjang dan lebar jari.
- **Pola retina:** Pola yang dibentuk oleh pembuluh darah di bawah permukaan retina adalah unik dan oleh karena itu cocok untuk identifikasi. Sistem biometrik retina memperoleh gambar digital dari pola retina dengan memproyeksikan sinar cahaya visual atau inframerah berintensitas rendah ke dalam mata.
- **Iris:** Karakteristik fisik unik lainnya yaitu, struktur iris mata yang mendetail.
- **Tanda tangan:** Setiap individu memiliki gaya tulisan tangan yang unik dan hal ini tercermin terutama dalam tanda tangan, yang biasanya merupakan urutan yang sering ditulis. Namun demikian, beberapa sampel tanda tangan dari satu individu tidak akan identik. Hal ini mempersulit tugas untuk mengembangkan representasi komputer dari tanda tangan yang dapat dicocokkan dengan sampel di masa depan.
- **Suara:** Sementara gaya khas seseorang tidak hanya mencerminkan atribut fisik yang unik dari penulisnya, tetapi juga kebiasaan menulis yang telah berkembang, pola suara lebih terkait erat dengan karakter fisik dan anatomi.

tics dari pembicara. Namun demikian, masih terdapat variasi dari sampel ke sampel dari waktu ke waktu dari pembicara yang sama, sehingga mempersulit tugas pengenalan biometrik.

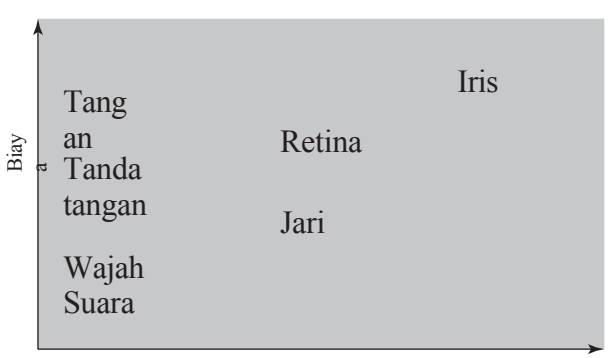
Gambar 3.7 memberikan indikasi kasar mengenai biaya relatif dan akurasi dari langkah-langkah biometrik ini. Konsep akurasi tidak berlaku pada skema autentikasi pengguna yang menggunakan kartu pintar atau kata sandi. Sebagai contoh, jika pengguna memasukkan kata sandi, kata sandi tersebut bisa sama persis dengan kata sandi yang diharapkan untuk pengguna tersebut atau tidak. Dalam kasus parameter biometrik, sistem harus menentukan seberapa dekat karakteristik biometrik yang ditampilkan cocok dengan karakteristik yang tersimpan. Sebelum menguraikan konsep akurasi biometrik, kita perlu memiliki gambaran umum tentang bagaimana sistem biometrik bekerja.

Pengoperasian Sistem Otentikasi Biometrik

Gambar 3.8 mengilustrasikan pengoperasian sistem biometrik. Setiap individu yang akan dimasukkan ke dalam basis data pengguna yang berwenang harus terlebih dahulu **terdaftar** dalam sistem. Hal ini serupa dengan pemberian kata sandi kepada pengguna. Untuk sistem biometrik, pengguna memberikan nama dan, biasanya, beberapa jenis kata sandi atau PIN ke sistem. Pada saat yang sama, sistem merasakan beberapa karakteristik biometrik dari pengguna ini (misalnya, sidik jari telunjuk kanan). Sistem mendigitalkan input dan kemudian mengekstrak satu set fitur yang dapat disimpan sebagai angka atau serangkaian angka yang mewakili karakteristik biometrik yang unik ini; serangkaian angka ini disebut sebagai template pengguna. Pengguna sekarang terdaftar dalam sistem, yang menyimpan nama (ID), mungkin PIN atau kata sandi, dan nilai biometrik.

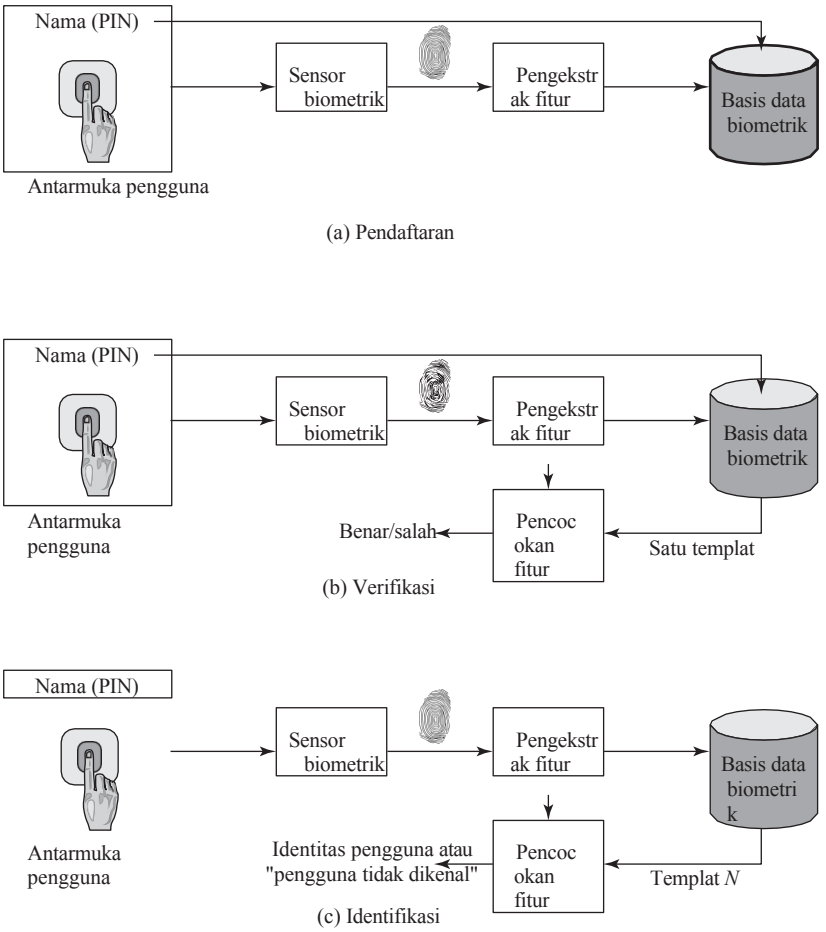
Tergantung pada aplikasinya, autentikasi pengguna pada sistem biometrik melibatkan **verifikasi** atau **identifikasi.** Verifikasi dianalogikan dengan pengguna yang masuk ke sistem dengan menggunakan kartu memori atau kartu pintar yang digabungkan dengan kata sandi atau PIN. Untuk verifikasi biometrik, pengguna memasukkan PIN dan juga menggunakan sensor biometrik. Sistem mengekstrak fitur yang sesuai dan membandingkannya dengan template yang disimpan untuk pengguna ini. Jika ada kecocokan, maka sistem akan mengautentikasi pengguna ini.

Untuk sistem identifikasi, individu menggunakan sensor biometrik tetapi tidak memberikan informasi tambahan. Sistem kemudian membandingkan templat yang disajikan dengan kumpulan templat yang tersimpan. Jika ada kecocokan, maka pengguna tersebut diidentifikasi. Jika tidak, maka pengguna ditolak.



Akurasi

Gambar 3.7 Biaya versus Akurasi Berbagai Karakteristik Biometrik dalam Skema Otentikasi Pengguna



Gambar 3.8 Sistem Biometrik Umum Pendaftaran menciptakan h u b u n g a n antara pengguna dan karakteristik biometrik pengguna. Tergantung pada aplikasinya, autentikasi pengguna melibatkan verifikasi bahwa pengguna yang diklaim adalah pengguna yang sebenarnya atau mengidentifikasi pengguna yang tidak dikenal.

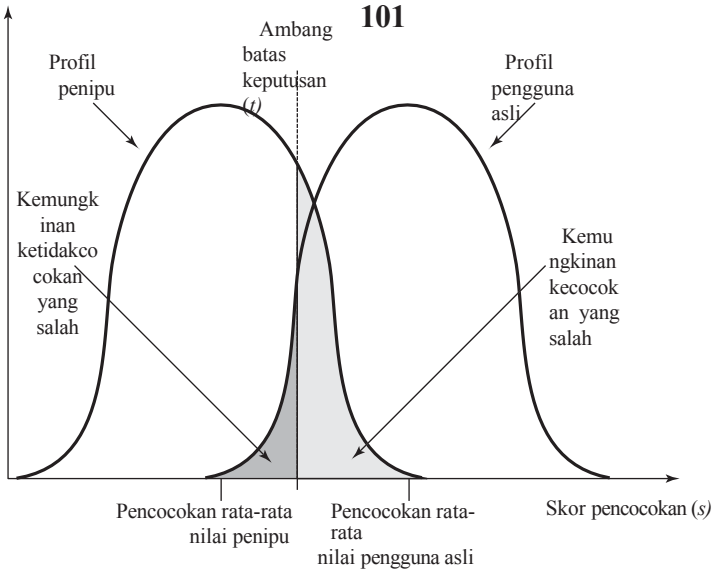
Akurasi Biometrik

Dalam skema biometrik apa pun, beberapa karakteristik fisik individu dipetakan ke dalam representasi digital. Untuk setiap individu, satu representasi digital, atau template, disimpan dalam komputer. Ketika pengguna akan diautentikasi, sistem membandingkan template yang tersimpan dengan template yang ditampilkan. Mengingat kompleksitas karakteristik fisik, kita tidak dapat berharap bahwa akan ada kecocokan yang tepat antara kedua template. Sebaliknya, sistem menggunakan algoritme untuk menghasilkan skor pencocokan (biasanya berupa angka tunggal) yang mengukur kesamaan antara input dan templat yang tersimpan. Untuk melanjutkan pembahasan, kami mendefinisikan istilah-istilah berikut ini. Tingkat kecocokan palsu adalah frekuensi sampel biometrik dari sumber yang berbeda dinilai secara keliru berasal dari sumber yang sama. Tingkat ketidakcocokan palsu adalah frekuensi sampel dari sumber yang sama dinilai secara keliru berasal dari sumber yang berbeda.

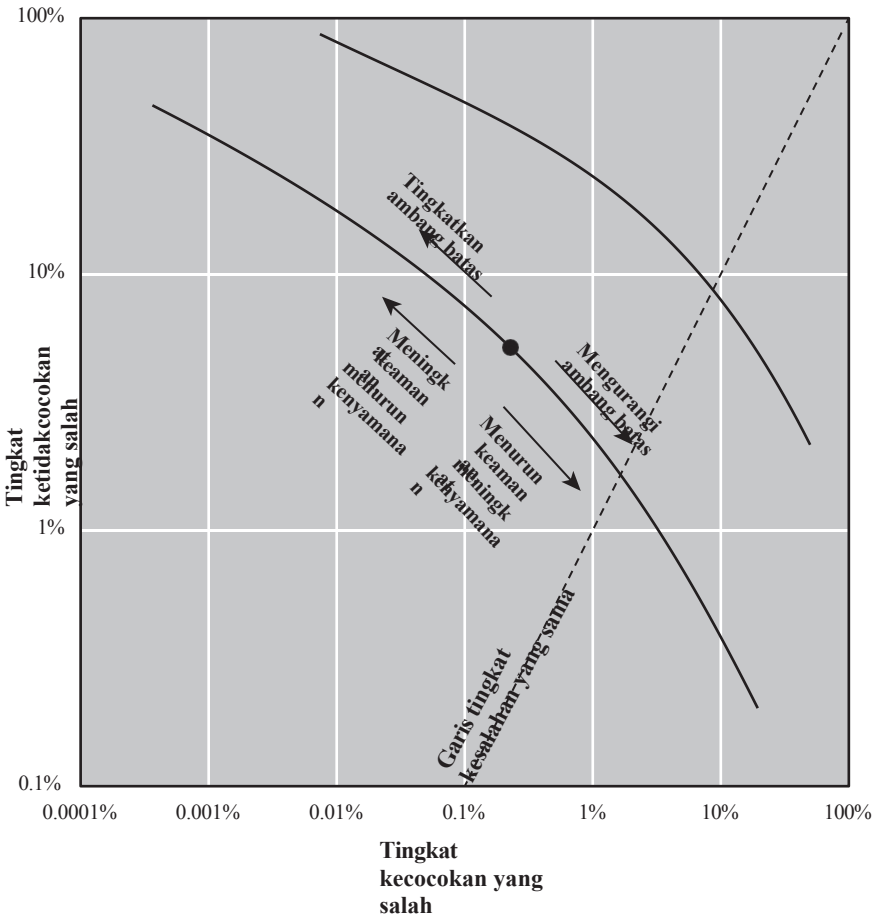
Gambar 3.9 mengilustrasikan dilema yang ditimbulkan pada sistem. Jika satu pengguna diuji oleh sistem berkali-kali, skor pencocokan akan bervariasi, dengan fungsi kepadatan probabilitas yang biasanya membentuk kurva lonceng, seperti yang ditunjukkan. Sebagai contoh, dalam kasus sidik jari, hasilnya dapat bervariasi karena kebisingan sensor; perubahan pada sidik jari karena membengkak atau kering; penempatan jari; dan sebagainya. Secara rata-rata, setiap individu lain seharusnya memiliki skor pencocokan yang jauh lebih rendah, tetapi sekali lagi akan menunjukkan fungsi kepadatan probabilitas berbentuk lonceng. Kesulitannya adalah bahwa rentang nilai pencocokan yang dihasilkan oleh dua individu, satu individu asli dan satu individu penipu, dibandingkan dengan template referensi yang diberikan, kemungkinan besar akan saling tumpang tindih. Pada Gambar 3.9, nilai ambang batas dipilih sedemikian rupa sehingga jika nilai yang ditampilkan s t diasumsikan sebagai kecocokan, dan untuk s t, diasumsikan tidak cocok. Bagian yang diarsir di sebelah kanan t menunjukkan rentang nilai yang memungkinkan terjadinya kecocokan palsu, dan bagian yang diarsir di sebelah kiri menunjukkan rentang nilai yang memungkinkan terjadinya ketidakcocokan palsu. Kecocokan palsu menghasilkan penerimaan pengguna yang seharusnya tidak diterima, dan ketidakcocokan palsu memicu penolakan pengguna yang valid. Area setiap bagian yang diarsir mewakili probabilitas kecocokan palsu atau ketidakcocokan. Dengan memindahkan ambang batas ke kiri atau ke kanan, probabilitas dapat diubah, tetapi perhatikan bahwa penurunan tingkat kecocokan palsu menghasilkan peningkatan tingkat ketidakcocokan palsu, dan sebaliknya.

Untuk skema biometrik yang diberikan, kita dapat memplot tingkat kecocokan palsu versus ketidakcocokan palsu, yang disebut kurva karakteristik operasi. Gambar 3.10 menunjukkan kurva ideal untuk dua sistem yang berbeda. Kurva yang lebih rendah dan ke kiri berkinerja lebih baik. Titik pada kurva sesuai dengan ambang batas tertentu untuk pengujian biometrik. Menggeser ambang batas di sepanjang kurva ke atas dan ke kiri memberikan keamanan yang lebih besar dan biaya yang lebih rendah. Ketidaknyamanan ini berasal dari pengguna yang sah yang ditolak aksesnya

Fungsi
kepadatan
probabilitas



Gambar 3.9 Profil Karakteristik Biometrik Penipu dan Pengguna Resmi Dalam penggambaran ini, perbandingan antara fitur yang ditampilkan dan fitur referensi direduksi menjadi nilai numerik tunggal. Jika nilai input (*s*) lebih besar dari ambang batas yang telah ditentukan sebelumnya (*t)*, sebuah kecocokan dinyatakan.



Gambar 3.10 Kurva Karakteristik Operasi Pengukuran Biometrik yang Diidealkan (skala log-log)

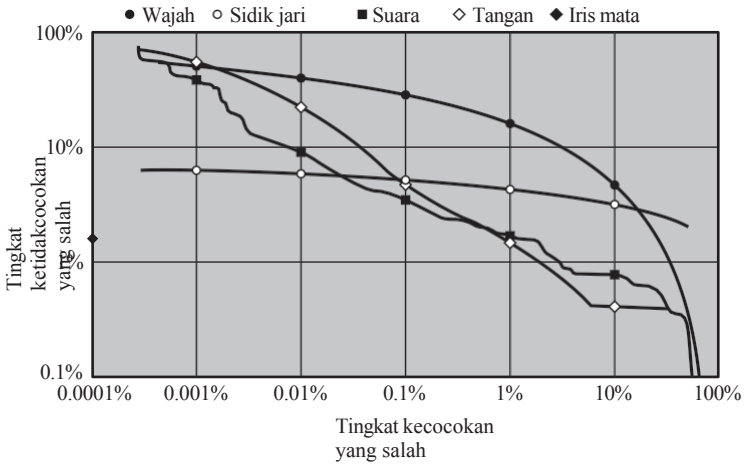
dan diminta untuk mengambil langkah lebih lanjut. Pengorbanan yang masuk akal adalah memilih ambang batas yang sesuai dengan titik pada kurva di mana tingkatnya sama. Aplikasi dengan keamanan tinggi mungkin memerlukan tingkat kecocokan palsu yang sangat rendah, sehingga menghasilkan titik yang lebih jauh ke kiri pada kurva. Untuk aplikasi forensik, di mana sistem mencari kandidat yang mungkin, untuk diperiksa lebih lanjut, persyaratannya mungkin tingkat ketidakcocokan palsu yang rendah.

Gambar 3.11 menunjukkan kurva karakteristik yang dikembangkan dari pengujian produk yang sesungguhnya. Sistem iris mata tidak memiliki kecocokan palsu dalam lebih dari 2 juta perbandingan silang. Perhatikan bahwa pada rentang tingkat kecocokan palsu yang luas, biometrik wajah adalah yang terburuk.

3. 5 OTENTIKASI PENGGUNA JARAK JAUH

Bentuk autentikasi pengguna yang paling sederhana adalah autentikasi lokal, di

mana pengguna mencoba mengakses sistem yang ada secara lokal, seperti PC kantor yang berdiri sendiri atau mesin ATM. Kasus yang lebih kompleks adalah autentikasi pengguna jarak jauh,



Gambar 3.11 Kurva Karakteristik Operasi Pengukuran Biometrik Aktual, Dilaporkan dalam [MANSO1] Untuk memperjelas perbedaan di antara sistem, skala log-log digunakan.

yang berlangsung melalui Internet, jaringan, atau sambungan komunikasi. Otentikasi pengguna jarak jauh menimbulkan ancaman keamanan tambahan, seperti penyadap yang dapat menangkap kata sandi, atau musuh yang mengulang urutan otentikasi yang telah diamati.

Untuk melawan ancaman terhadap autentikasi pengguna jarak jauh, sistem umumnya mengandalkan beberapa bentuk protokol tantangan-tanggapan. Pada bagian ini, kami menyajikan elemen dasar dari protokol tersebut untuk setiap jenis autentikator yang dibahas dalam bab ini.

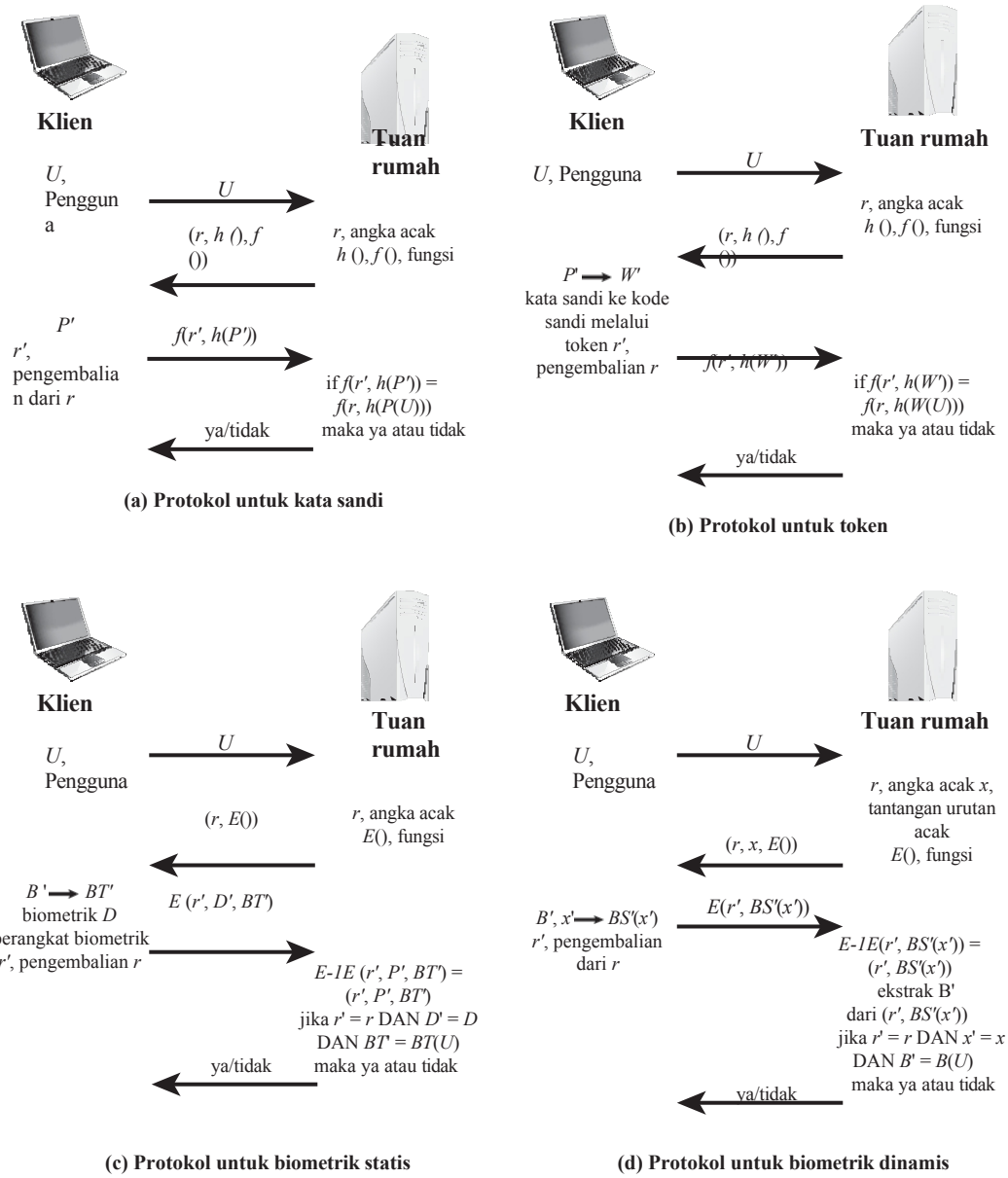
Protokol Kata Sandi

Gambar 3.12a menyediakan contoh sederhana dari protokol tantangan-respons untuk autentikasi melalui kata sandi. Protokol yang sebenarnya lebih kompleks, seperti Kerberos, yang dibahas di Bab 23. Pada contoh ini, pengguna pertama-tama mengirimkan identitasnya ke remote host. Host menghasilkan angka acak r, sering disebut **nonce**, dan mengembalikan nonce ini ke pengguna. Selain itu, host menentukan dua fungsi, h() dan f(), yang akan digunakan dalam respons. Transmisi dari host ke pengguna inilah yang menjadi tantangan. Tanggapan dari pengguna adalah kuantitas f(r', h(P')), di mana r' r dan P' adalah kata sandi pengguna. Fungsi h adalah sebuah fungsi hash, sehingga respon terdiri dari fungsi hash dari kata sandi pengguna yang digabungkan dengan angka acak menggunakan fungsi f.

Host menyimpan fungsi hash dari setiap kata sandi pengguna yang terdaftar, digambarkan sebagai h($P(U)$) untuk pengguna U. Ketika respons tiba, host membandingkan f(r', h(P')) yang masuk dengan f(r, h($P(U)$) yang telah dihitung.) Jika jumlahnya cocok, pengguna diautentikasi.

Skema ini melindungi dari beberapa bentuk serangan. Host tidak menyimpan kata sandi tetapi kode hash dari kata sandi. Seperti yang dibahas pada Bagian 3.2, hal ini mengamankan kata sandi dari penyusup ke dalam sistem host. Sebagai tambahan, bahkan hash kata sandi tidak dikirimkan secara langsung, melainkan sebuah fungsi dimana hash kata sandi merupakan salah satu argumen. Dengan demikian, untuk

fungsi f yang sesuai, hash kata sandi tidak dapat dibatasi selama transmisi. Terakhir, penggunaan nomor acak sebagai salah satu argumen



Gambar 3.12 Protokol Tantangan-Tanggapan Dasar untuk Otentikasi Pengguna Jarak Jauh
Sumber: Berdasarkan [OGOR03].

dari f bertahan dari serangan replay, di mana musuh menangkap transmisi pengguna dan mencoba untuk masuk ke sistem dengan mentransmisikan ulang pesan pengguna.

Protokol Token

Gambar 3.12b memberikan contoh sederhana protokol token untuk autentikasi. Seperti sebelumnya, pengguna pertama-tama mengirimkan identitasnya ke remote host. Host mengembalikan sebuah angka acak dan pengenal fungsi f() dan h() untuk digunakan dalam fungsi

respon. Di sisi pengguna, token menyediakan kode sandi W'. Token menyimpan kode sandi statis atau menghasilkan kode sandi acak satu kali. Untuk kode sandi acak satu kali, token harus disinkronkan dengan cara tertentu dengan host. Dalam kedua kasus tersebut, pengguna mengaktifkan kode sandi dengan memasukkan kata sandi P'. Kata sandi ini hanya dibagikan antara pengguna dan token dan tidak melibatkan host jarak jauh. Token merespons host dengan kuantitas f(r', h(W')). Untuk kode sandi statis, host menyimpan nilai hash h($W(U)$); untuk kode sandi dinamis, host membuat kode sandi satu kali (disinkronkan dengan yang dibuat oleh token) dan mengambil hash-nya. Otentikasi kemudian dilanjutkan dengan cara yang sama seperti protokol kata sandi.

Protokol Biometrik Statis

Gambar 3.12c adalah contoh protokol autentikasi pengguna menggunakan biometrik statis. Seperti sebelumnya, pengguna mengirimkan ID ke host, yang merespon dengan sebuah angka acak r dan, dalam hal ini, pengenal untuk enkripsi E(). Di sisi pengguna terdapat sebuah sistem klien tem yang mengontrol perangkat biometrik. Sistem ini menghasilkan sebuah template biometrik BT' dari biometrik pengguna B' dan mengembalikan ciphertext E(r', D', BT'), *di* mana D' mengidentifikasi perangkat biometrik tertentu. Host mendekripsi pesan yang masuk untuk memulihkan tiga parameter yang dikirimkan dan membandingkannya dengan nilai yang tersimpan secara lokal. Agar cocok, host harus menemukan $r' = r$. Selain itu, nilai kecocokan antara BT' dan template yang tersimpan harus melebihi ambang batas yang telah ditentukan. Terakhir, host menyediakan otentikasi sederhana untuk perangkat perekam biometrik dengan membandingkan ID perangkat yang masuk dengan daftar perangkat yang terdaftar di basis data host.

Protokol Biometrik Dinamis

Gambar 3.12d adalah contoh protokol autentikasi pengguna yang menggunakan biometrik dinamis. Perbedaan utama dari kasus biometrik stabil adalah bahwa host menyediakan urutan acak serta nomor acak sebagai tantangan. Tantangan urutan adalah urutan angka, karakter, atau kata. Pengguna manusia di sisi klien kemudian harus menyuarakan (verifikasi pembicara), mengetik (verifikasi dinamika keyboard), atau menulis (verifikasi tulisan tangan) urutan tersebut untuk menghasilkan sinyal biometrik $BS'(x')$. Sisi klien mengenkripsi sinyal biometrik dan nomor acak. Di sisi host, pesan yang masuk didekripsi. Angka acak yang masuk r' harus sama persis dengan angka acak yang awalnya digunakan sebagai tantangan (r). Selain itu, host membuat perbandingan berdasarkan sinyal biometrik yang masuk $BS'(x')$, template yang tersimpan $BT(U)$ untuk pengguna ini dan sinyal asli x. Jika nilai perbandingan melebihi ambang batas yang telah ditentukan, pengguna diautentikasi.

3. 6 MASALAH KEAMANAN UNTUK AUTENTIKASI PENGGUNA

Seperti halnya layanan keamanan lainnya, autentikasi pengguna, terutama

autentikasi pengguna jarak jauh, dapat diserang dengan berbagai macam serangan. Tabel 3.4, dari [OGOR03], meringkas serangan utama pada autentikasi pengguna, yang dibagi berdasarkan jenis autentikator. Sebagian besar dari tabel ini sudah cukup jelas. Pada bagian ini, kita akan mengembangkan beberapa entri dari tabel tersebut.

Tabel 3.4 Beberapa Potensi Serangan, Autentikator yang Rentan, dan Pertahanan Umum

Serangan	Pengesah	Contoh	Pertahanan Khas
Serangan klien	Kata sandi	Menebak-nebak, pencarian yang melelahkan	Entropi besar; upaya terbatas
	Token	Pencarian lengkap	Entropi besar; upaya terbatas; pencurian objek membutuhkan kehadiran
	Biometrik	Kecocokan yang salah	Entropi besar; upaya terbatas
Serangan tuan rumah	Kata sandi	Pencurian teks biasa, pencarian kamus/pengelusuran lengkap	Hashing; entropi yang besar; perlindungan basis data kata sandi
	Token	Pencurian kode sandi	Sama seperti kata sandi; kode sandi 1 kali
	Biometrik	Pencurian templat	Menangkap otentikasi perangkat; respons tantangan
Menguping, pencurian, dan menyalin	Kata sandi	"Berselancar di atas bahu"	Ketekunan pengguna untuk menjaga rahasia; ketekunan administrator untuk dengan cepat mencabut kata sandi yang disalahgunakan; autentikasi multifaktor
	Token	Pencurian, pemalsuan perangkat keras	Otentikasi multifaktor; token yang tahan terhadap kerusakan/bukti
	Biometrik	Menyalin (memalsukan) biometrik	Deteksi penyalinan pada perangkat penangkap dan autentikasi perangkat penangkap
Putar ulang	Kata sandi	Memutar ulang respons kata sandi yang dicuri	Protokol tanggapan-tantangan
	Token	Memutar ulang respons kode sandi yang dicuri	Protokol respons tantangan; kode sandi 1 kali
	Biometrik	Memutar ulang respons templat biometrik yang dicuri	Deteksi penyalinan pada perangkat tangkap dan autentikasi perangkat tangkap melalui protokol respons tantangan
Kuda Troya	Kata sandi, token, biometrik	Pemasangan klien nakal atau perangkat penangkap	Otentikasi klien atau perangkat pengambilan dalam perimeter keamanan tepercaya
Penolakan layanan	Kata sandi, token, biometrik	Penguncian oleh beberapa otentikasi yang gagal	Multifaktor dengan token

Serangan klien adalah **serangan** di mana musuh mencoba untuk mencapai

autentikasi pengguna tanpa akses ke host jarak jauh atau ke jalur komunikasi yang mengintervensi. Musuh mencoba untuk menyamar sebagai pengguna yang sah. Untuk sistem berbasis kata sandi, musuh mungkin mencoba menebak kata sandi pengguna yang mungkin. Beberapa tebakan dapat dilakukan. Secara ekstrim, musuh mengurutkan semua kata sandi yang mungkin dalam upaya yang menyeluruh untuk berhasil. Salah satu cara untuk menggagalkan serangan seperti itu adalah dengan memilih kata sandi yang panjang dan tidak bisa ditebak. Efeknya,

kata sandi seperti itu memiliki entropi yang besar; yaitu, banyak bit yang diperlukan untuk mewakili kata sandi. Tindakan pencegahan lainnya adalah dengan membatasi jumlah percobaan yang dapat dilakukan dalam periode waktu tertentu dari sumber tertentu.

Sebuah token dapat menghasilkan sebuah kode sandi dengan entropi tinggi dari PIN atau kata sandi dengan entropi rendah, sehingga menggagalkan pencarian yang mendalam. Musuh mungkin dapat menebak atau mendapatkan PIN atau kata sandi, namun juga harus mendapatkan token fisik untuk berhasil.

Serangan host diarahkan pada file pengguna di host tempat kata sandi, kode sandi token, atau templat biometrik disimpan. Bagian 3.2 membahas pertimbangan keamanan sehubungan dengan kata sandi. Untuk token, ada pertahanan tambahan dengan menggunakan kode sandi satu kali, sehingga kode sandi tidak disimpan di file kode sandi host. Fitur biometrik dari seorang pengguna sulit untuk diamankan karena merupakan fitur fisik dari pengguna. Untuk fitur statis, otentikasi perangkat biometrik menambahkan ukuran perlindungan. Untuk fitur dinamis, protokol respons-tantangan meningkatkan keamanan.

Menguping dalam konteks kata sandi mengacu pada upaya musuh untuk mempelajari kata sandi dengan mengamati pengguna, menemukan salinan tertulis dari kata sandi, atau beberapa serangan serupa yang melibatkan kedekatan fisik antara pengguna dan musuh. Bentuk lain dari penyadapan adalah pencatatan keystroke (keylogging), di mana perangkat keras atau perangkat lunak berbahaya dipasang sehingga penyerang dapat menangkap keystroke pengguna untuk dianalisis kemudian. Sebuah sistem yang bergantung pada beberapa faktor (misalnya, kata sandi plus token atau kata sandi plus biometrik) tahan terhadap jenis serangan ini. Untuk sebuah token, ancaman yang serupa adalah **pencurian** token atau penyalinan fisik token. Sekali lagi, protokol multifaktor lebih tahan terhadap jenis serangan ini daripada protokol token murni. Ancaman analog untuk protokol biometrik adalah **menyalin** atau meniru parameter biometrik untuk menghasilkan template yang diinginkan. Biometrik dinamis tidak terlalu rentan terhadap serangan semacam itu. Untuk biometrik statis, otentikasi perangkat adalah tindakan pencegahan yang berguna.

Serangan **replay** melibatkan musuh yang mengulangi respons pengguna yang ditangkap sebelumnya. Penanggulangan yang paling umum untuk serangan semacam itu adalah protokol respons tantangan.

Dalam serangan **Trojan horse**, sebuah aplikasi atau perangkat fisik menyamar sebagai aplikasi atau perangkat otentik dengan tujuan menangkap kata sandi, kode sandi, atau biometrik pengguna. Musuh kemudian dapat menggunakan informasi yang ditangkap untuk menyamar sebagai pengguna yang sah. Contoh sederhana dari hal ini adalah mesin bank jahat yang digunakan untuk menangkap kombinasi ID pengguna/kata sandi.

Serangan **penolakan layanan** mencoba untuk menonaktifkan layanan otentikasi pengguna dengan membanjiri layanan dengan banyak percobaan otentikasi. Serangan yang lebih selektif menolak layanan untuk pengguna tertentu dengan mencoba masuk sampai ambang batas tercapai yang menyebabkan penguncian pada pengguna ini karena terlalu banyak percobaan masuk. Protokol autentikasi multifacet yang menyertakan token menggagalkan serangan ini, karena musuh harus mendapatkan token terlebih dahulu.

3.7 APLIKASI PRAKTIS: SISTEM BIOMETRIK IRIS

Sebagai contoh sistem autentikasi pengguna biometrik, kami melihat sistem biometrik iris mata yang dikembangkan untuk digunakan oleh Uni Emirat Arab (UEA) pada titik kontrol perbatasan [DAUG04, TIRO05, NBSP08]. UEA sangat bergantung pada tenaga kerja dari luar, dan semakin menjadi daya tarik wisata. Dengan demikian,

relatif terhadap ukurannya, UEA memiliki volume pengunjung yang sangat besar. Pada hari biasa, lebih dari 6.500 penumpang memasuki UEA melalui tujuh bandara internasional, tiga pelabuhan darat, dan tujuh pelabuhan laut. Menangani volume besar pengunjung yang masuk dengan cara yang efisien dan tepat waktu dengan demikian menimbulkan tantangan keamanan yang signifikan. Yang menjadi perhatian khusus UEA adalah upaya orang-orang yang diusir untuk masuk kembali ke negara ini. Cara tradisional untuk mencegah masuknya kembali orang yang diusir adalah dengan mengidentifikasi individu berdasarkan nama, tanggal lahir, dan data berbasis teks lainnya. Risikonya adalah informasi ini dapat diubah setelah pengusiran. Seseorang dapat datang dengan paspor yang berbeda dengan kewarganegaraan yang berbeda dan perubahan pada informasi identifikasi lainnya.

Untuk mengatasi upaya tersebut, UEA memutuskan untuk menggunakan sistem identifikasi biometrik dan mengidentifikasi persyaratan berikut:

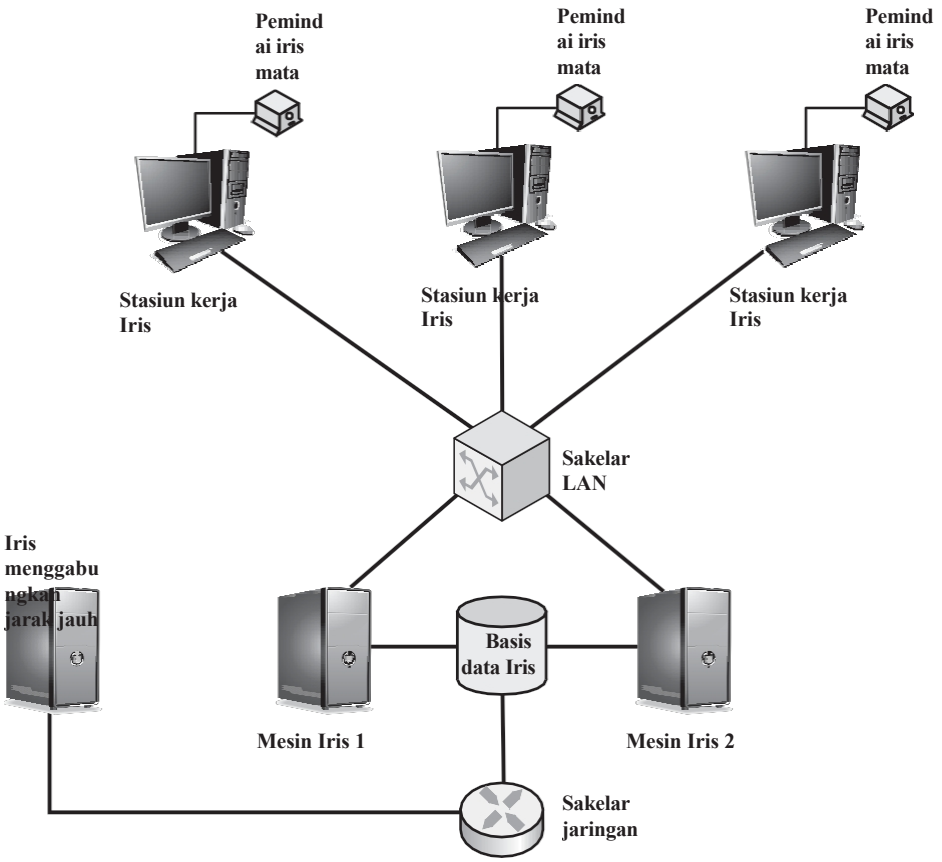
- Mengidentifikasi satu orang dari sekumpulan besar orang
- Mengandalkan fitur biometrik yang tidak berubah seiring waktu
- Gunakan fitur biometrik yang dapat diperoleh dengan cepat
- Mudah digunakan
- Menanggapi secara real-time untuk aplikasi angkutan massal
- Aman dan non-invasif
- Skala ke dalam miliaran perbandingan dan pertahankan kinerja terbaik
- Terjangkau

Dan memilih pengenalan iris mata sebagai metode yang paling efisien dan sangat mudah. Tidak ada dua iris mata yang sama. Tidak ada korelasi antara pola iris mata kembar identik sekalipun, atau mata kanan dan kiri seseorang.

Implementasi sistem melibatkan pendaftaran dan pemeriksaan identitas. Semua orang asing yang diusir harus menjalani pemindaian iris mata di salah satu dari beberapa pusat pendaftaran. Informasi ini digabungkan ke dalam satu basis data pusat. Pemindai iris mata dipasang di semua 17 pelabuhan udara, darat, dan laut yang masuk ke UEA. Kamera pengenal iris mata mengambil gambar hitam-putih dengan jarak 5 hingga 24 inci dari mata, tergantung pada kameranya. Kamera ini menggunakan pencahayaan inframerah-dekat non-invasif yang mirip dengan remote control TV, nyaris tidak terlihat dan dianggap sangat aman. Gambar pertama diproses oleh perangkat lunak yang melokalisasi batas dalam dan luar iris, dan kontur kelopak mata, untuk mengekstrak bagian iris saja. Perangkat lunak ini menciptakan apa yang disebut kode fase untuk tekstur iris mata, mirip dengan kode urutan DNA. Fitur unik dari iris mata ditangkap oleh kode ini dan dapat dibandingkan dengan basis data besar iris mata yang dipindai untuk membuat kecocokan. Melalui jaringan terdistribusi (Gambar 3.13), kode iris mata dari semua penumpang yang datang dibandingkan secara real time dengan database pusat yang terdaftar.

Perlu diketahui bahwa ini adalah tugas yang lebih berat secara komputasi daripada memverifikasi identitas. Dalam hal ini, pola iris mata setiap penumpang yang masuk dibandingkan dengan seluruh basis data pola yang telah diketahui untuk menentukan apakah ada kecocokan. Dengan volume lalu lintas dan ukuran basis data saat ini, jumlah perbandingan silang iris mata setiap hari mencapai lebih dari 9 miliar.

Seperti halnya sistem keamanan lainnya, musuh selalu mencari cara untuk menangkalnya. Para pejabat UEA harus mengadopsi metode keamanan baru untuk mendeteksi apakah iris mata telah dilebarkan dengan obat tetes mata sebelum melakukan pemindaian. Ekspatriat yang dilarang masuk ke



Gambar 3.13 **Arsitektur Situs Pemindaian Iris Umum untuk Sistem UEA**

UEA mulai menggunakan obat tetes mata dalam upaya mengelabui sistem pengenalan iris mata pemerintah ketika mereka mencoba masuk kembali ke negara tersebut. Sebuah algoritme baru dan prosedur langkah demi langkah terkomputerisasi telah diadopsi untuk membantu para petugas menentukan apakah iris mata dalam kondisi normal atau obat tetes mata telah digunakan.

3.8 STUDI KASUS : MASALAH KEAMANAN SISTEM ATM

Redspin, Inc., sebuah auditor independen, baru-baru ini mengeluarkan sebuah laporan yang menjelaskan kerentanan keamanan dalam penggunaan ATM (Anjungan Tunai Mandiri) yang mempengaruhi sejumlah penerbit kartu ATM skala kecil hingga menengah. Kerentanan ini memberikan sebuah studi kasus yang berguna untuk menggambarkan bahwa fungsi dan layanan kriptografi saja tidak menjamin keamanan; mereka harus diimplementasikan dengan baik sebagai bagian dari sebuah sistem.

Kami mulai dengan mendefinisikan istilah yang digunakan dalam bagian ini:

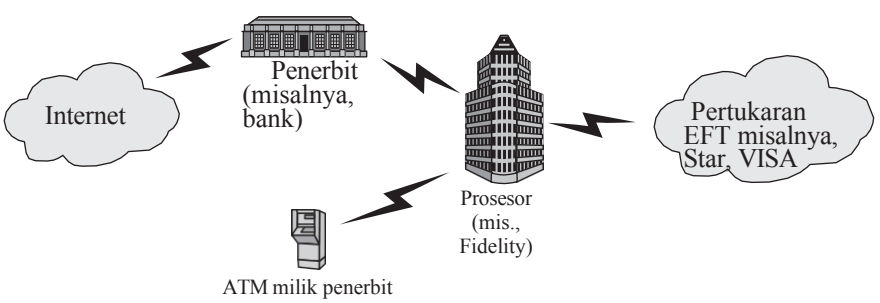
- **Pemegang kartu:** Individu yang menerima kartu debit. Biasanya, individu

ini juga bertanggung jawab atas pembayaran semua tagihan yang dilakukan pada kartu tersebut.

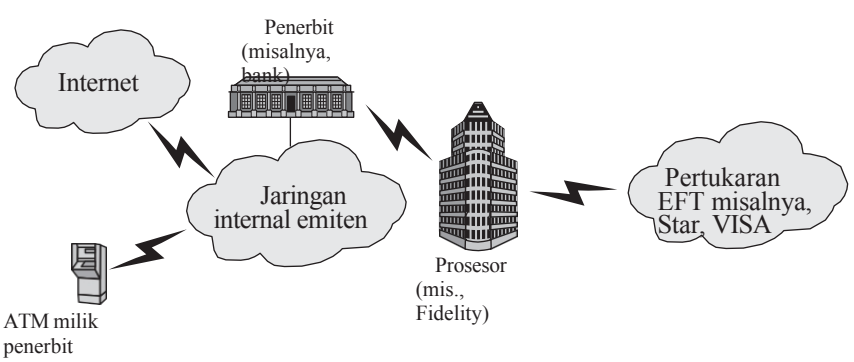
- **Penerbit:** Institusi yang menerbitkan kartu debit kepada pemegang kartu. Lembaga ini bertanggung jawab atas rekening pemegang kartu dan mengesahkan semua transaksi. Bank dan serikat kredit adalah penerbit yang umum.
- **Pemroses:** Organisasi yang menyediakan layanan seperti pemrosesan data inti (pengenalan PIN dan pembaruan akun), transfer dana elektronik (EFT), dan sebagainya kepada penerbit. EFT memungkinkan penerbit untuk mengakses jaringan regional dan nasional yang menghubungkan perangkat point of sale (POS) dan ATM di seluruh dunia. Contoh perusahaan yang melakukan proses ini antara lain Fidelity National Financial dan Jack Henry & Associates.

Nasabah mengharapkan layanan 24 jam sehari, 7 hari seminggu di stasiun ATM. Bagi banyak penerbit kecil hingga menengah, akan lebih hemat biaya jika pemroses kontrak menyediakan pemrosesan data dan layanan EFT/ATM yang diperlukan. Setiap layanan biasanya membutuhkan koneksi data khusus antara penerbit dan prosesor, menggunakan leased line atau virtual leased line.

Sebelum sekitar tahun 2003, konfigurasi umum yang melibatkan penerbit, prosesor, dan mesin ATM dapat dicirikan oleh Gambar 3.14a. Unit ATM terhubung langsung ke prosesor dan bukannya ke penerbit yang memiliki ATM, melalui leased line atau virtual leased line. Penggunaan sambungan khusus menyulitkan untuk melakukan kejahatan.



(a) Sambungan point-to-point ke prosesor



(b) Sambungan bersama ke prosesor

Gambar 3.14 Arsitektur ATM Sebagian besar penerbit kartu debit skala kecil

hingga menengah menggunakan prosesor untuk menyediakan pemrosesan data inti dan layanan transfer dana elektronik (EFT). Mesin ATM bank dapat terhubung langsung ke prosesor atau ke bank.

mencegat data yang ditransfer. Untuk menambah keamanan, bagian PIN dari pesan yang dikirimkan dari ATM ke prosesor dienkripsi menggunakan DES (Standar Enkripsi Data). Prosesor memiliki koneksi ke jaringan pertukaran EFT (transfer dana elektronik) untuk memungkinkan pemegang kartu mengakses rekening dari ATM mana pun. Dengan konfigurasi Gambar 3.14a, sebuah transaksi berlangsung sebagai berikut. Pengguna menggesek kartunya dan memasukkan PIN. ATM mengenkripsi PIN dan mengirimkannya ke prosesor sebagai bagian dari permintaan otorisasi. Pemroses memperbarui informasi pelanggan dan mengirimkan balasan.

Pada awal tahun 2000-an, bank-bank di seluruh dunia memulai proses migrasi dari ATM generasi lama yang menggunakan sistem operasi OS/2 IBM ke sistem baru yang menggunakan Windows. Migrasi massal ke Windows didorong oleh sejumlah faktor, termasuk keputusan IBM untuk berhenti mendukung OS/2 pada tahun 2006, tekanan pasar dari kreditor seperti MasterCard International dan Visa International untuk memperkenalkan Triple DES yang lebih kuat, dan tekanan dari regulator AS untuk memperkenalkan fitur baru bagi pengguna yang dinonaktifkan. Banyak bank, seperti yang diaudit oleh Redspin, menyertakan sejumlah peningkatan lain pada saat yang sama dengan pengenalan Windows dan triple DES, terutama penggunaan TCP / IP sebagai transportasi jaringan.

Karena penerbit biasanya menjalankan jaringan area lokal (LAN) dan intranet yang terhubung ke Internet menggunakan TCP/IP, maka sangat menarik untuk menghubungkan ATM ke jaringan penerbit ini dan hanya mempertahankan satu jalur khusus ke prosesor, yang mengarah ke konfigurasi yang diilustrasikan pada Gambar 3.14b. Konfigurasi ini menghemat biaya sirkuit bulanan yang mahal bagi penerbit dan memungkinkan pengelolaan ATM yang lebih mudah oleh penerbit. Dalam konfigurasi ini, informasi yang dikirim dari ATM ke prosesor melewati jaringan penerbit sebelum dikirim ke prosesor. Pada saat berada di jaringan penerbit inilah informasi nasabah menjadi rentan.

Masalah keamanannya adalah bahwa dengan peningkatan ke OS ATM baru dan konfigurasi komunikasi baru, satu-satunya peningkatan keamanan adalah penggunaan triple DES dan bukan DES untuk mengenkripsi PIN. Informasi lainnya dalam pesan permintaan ATM dikirim secara jelas. Ini termasuk nomor kartu, tanggal kedaluwarsa, saldo rekening, dan jumlah penarikan. Seorang peretas yang menyadap jaringan bank, baik dari lokasi internal maupun dari Internet berpotensi memiliki akses penuh ke setiap transaksi ATM.

Situasi yang baru saja dijelaskan mengarah pada dua kerentanan utama:

- **Kerahasiaan:** Nomor kartu, tanggal kedaluwarsa, dan saldo rekening dapat digunakan untuk pembelian online atau membuat kartu duplikat untuk transaksi berbasis tanda tangan.
- **Integritas:** Tidak ada perlindungan untuk mencegah penyerang menyuntikkan atau mengubah data dalam perjalanan. Jika penyerang dapat menangkap pesan dalam perjalanan, penyerang dapat menyamar sebagai prosesor atau ATM. Bertindak sebagai pemroses, penyerang dapat mengarahkan ATM untuk mengeluarkan uang tanpa pemroses mengetahui bahwa sebuah transaksi telah terjadi. Jika musuh menangkap informasi akun pengguna dan PIN terenkripsi, akun tersebut dikompromikan sampai kunci enkripsi ATM diubah, sehingga memungkinkan musuh untuk mengubah saldo akun atau melakukan transfer.

Redspin merekomendasikan sejumlah langkah yang dapat diambil bank untuk mengatasi ancaman ini. Perbaikan jangka pendek termasuk menyegmentasikan lalu lintas ATM dari lalu lintas

jaringan baik dengan menerapkan aturan firewall yang ketat atau secara fisik membagi jaringan sama sekali. Perbaikan jangka pendek tambahan adalah dengan menerapkan enkripsi tingkat jaringan antara router yang dilalui lalu lintas ATM.

Perbaikan jangka panjang melibatkan perubahan pada perangkat lunak tingkat aplikasi. Melindungi kerahasiaan memerlukan enkripsi semua informasi terkait nasabah yang melintasi jaringan. Memastikan integritas data memerlukan otentikasi mesin-ke-mesin yang lebih baik antara ATM dan prosesor serta penggunaan protokol tantangan-tanggapan untuk mengatasi serangan ulangan.

3. 9 Penghematan Energi

[OGOR03] adalah makalah yang perlu dibaca untuk survei otoritatif tentang topik-topik dalam bab ini. [BURR13] juga merupakan survei yang bermanfaat. [SCAR09] adalah sebuah pandangan yang komprehensif pada banyak masalah yang berhubungan dengan pemilihan dan manajemen kata sandi.

BURR13 Burr, W, dkk. *Pedoman Otentikasi Elektronik.* Gaithersburg, MD: National Institute of Standards and Technology, Publikasi Khusus 800-63-2, Agustus 2013.

OGOR03 O'Gorman, L. "Membandingkan Kata Sandi, Token, dan Biometrik untuk Otentikasi Pengguna." *Prosiding IEEE*, Desember 2003.

SCAR09a Scarfone, K., dan Souppaya, M. *Panduan untuk Manajemen Kata Sandi Perusahaan (Draft)*. Publikasi Khusus NIST SP 800-118 (Draft), April 2009.

3.10 TUJUAN U T A M A, PERTANYAAN-PERTANYAAN, DAN PERMASALAHAN

Istilah Kunci

biometrik	identifikasi	kartu pintar
protokol tantangan-tanggapan	kartu memori	biometrik statis
penuntut	nonce	pelanggan
kredensial	kata sandi	token
penyedia layanan kredensial (CSP)	meja pelangi	otentikasi pengguna
biometrik dinamis	otoritas pendaftaran (RA)	verifikasi
mendaftar	pihak yang diandalkan (RP)	verifikator
kata sandi terenkripsi	garam	
	file kata sandi bayangan	

Tinjau Pertanyaan

3.1 Secara umum, apa saja empat cara untuk mengautentikasi identitas pengguna?

3.2 Sebutkan dan jelaskan secara singkat ancaman utama terhadap kerahasiaan kata

sandi. **115**

3.3 Apa saja dua teknik umum yang digunakan untuk melindungi file kata sandi?

3.4 Sebutkan dan jelaskan secara singkat empat teknik umum untuk memilih atau menetapkan kata sandi.

3.5 Jelaskan perbedaan antara kartu memori sederhana dan kartu pintar.

3.6 Sebutkan dan jelaskan secara singkat ciri-ciri fisik utama yang digunakan untuk identifikasi biometrik.

3.7 Dalam konteks autentikasi pengguna biometrik, jelaskan istilah-istilah, pendaftaran, verifikasi, dan identifikasi.

3.8 Definisikan istilah *tingkat kecocokan palsu* dan *tingkat* ketidakcocokan *palsu,* dan jelaskan penggunaan ambang batas dalam kaitannya dengan kedua tingkat ini.

3.9 Jelaskan konsep umum dari protokol tantangan-tanggapan.

Masalah

3.1 Jelaskan kesesuaian atau ketidaksesuaian kata sandi berikut ini:

a. YK 334 b . mfmitm (untuk "film favorit saya c . Natalie1 d . Washington adalah belas kasihan yang lembut)

e. Aristoteles f . tv9kompor **g.** 1 2 3 4 5 6 7 8 **h.** dribgib

3.2 Upaya awal untuk memaksa pengguna menggunakan kata sandi yang tidak mudah ditebak adalah dengan menggunakan kata sandi yang disediakan oleh komputer. Kata sandi tersebut terdiri dari delapan karakter dan diambil dari kumpulan karakter yang terdiri dari huruf kecil dan angka. Kata sandi tersebut dihasilkan oleh generator angka acak semu dengan 2^{15} kemungkinan nilai awal. Dengan menggunakan teknologi pada saat itu, waktu yang dibutuhkan untuk mencari semua string karakter dengan panjang 8 dari alfabet 36 karakter adalah 112 tahun. Sayangnya, ini bukanlah gambaran yang sebenarnya dari keamanan sistem yang sebenarnya. Jelaskan masalahnya.

3.3 Asumsikan bahwa kata sandi dipilih dari kombinasi empat karakter yang terdiri dari 26 karakter alfa-betik. Asumsikan bahwa musuh dapat mencoba kata sandi dengan kecepatan satu per detik.

a. Dengan asumsi tidak ada umpan balik kepada pihak lawan sampai setiap upaya selesai, berapa waktu yang diharapkan untuk menemukan kata sandi yang benar?

b. Dengan asumsi umpan balik kepada pihak lawan yang menandai kesalahan saat setiap karakter yang salah dimasukkan, berapa lama waktu yang diharapkan untuk menemukan kata sandi yang benar?

3.4 Asumsikan bahwa elemen sumber dengan panjang k dipetakan dengan cara yang seragam ke dalam elemen target dengan panjang p. Jika setiap angka dapat mengambil salah satu dari nilai r, maka jumlah elemen sumber adalah r^k dan jumlah elemen target adalah angka yang lebih kecil, yaitu r^p . Sebuah elemen sumber tertentu x_i dipetakan ke elemen target tertentu y_j

a. Berapa probabilitas bahwa elemen sumber yang benar dapat dipilih oleh musuh dalam satu kali percobaan?

b. Berapa probabilitas bahwa sebuah elemen sumber yang berbeda x_k (x_i x_k) yang menghasilkan elemen target yang sama, yj, dapat diproduksi oleh musuh?

c. Berapa probabilitas bahwa elemen target yang benar dapat dihasilkan oleh musuh dalam satu kali percobaan?

3.5 Pembuat kata sandi fonetik mengambil dua segmen secara acak untuk setiap kata sandi enam huruf. Bentuk setiap segmen adalah CVC (konsonan, vokal, konsonan), di mana
V = 6 a, e, i, o, u 7 dan C V- .

a. Berapakah total populasi kata sandi?

b. Berapa probabilitas seorang musuh menebak kata sandi dengan benar?

3.6 Asumsikan bahwa kata sandi terbatas pada penggunaan 95 karakter ASCII yang dapat dicetak dan semua kata sandi terdiri dari 10 karakter. Asumsikan bahwa seorang peretas kata sandi memiliki kecepatan enkripsi 6,4 juta enkripsi per detik.

Berapa lama waktu yang dibutuhkan untuk menguji secara menyeluruh semua password yang mungkin pada sistem UNIX?

3.7 Karena resiko yang diketahui dari sistem password UNIX, dokumentasi SunOS-4.0 merekomendasikan agar file password dihapus dan digantikan dengan file yang dapat dibaca oleh publik yang disebut /etc/publickey. Entri pada berkas untuk user A terdiri dari *ID* pengenal user_A , kunci publik user, PU_a , dan kunci privat PR_a .

Kunci privat ini dienkripsi menggunakan DES dengan kunci yang berasal dari kata sandi masuk pengguna P_a . Ketika A masuk, sistem akan mendekripsi E (P_a , PR_a) untuk mendapatkan PR_a .

a. Sistem kemudian memverifikasi bahwa P_a diberikan dengan benar. Bagaimana?

b. Bagaimana lawan dapat menyerang sistem ini?

3.8 Disebutkan bahwa penyertaan salt di dalam skema kata sandi UNIX meningkatkan kesulitan menebak dengan faktor 4096. Tetapi salt disimpan dalam bentuk plaintext di entri yang sama dengan kata sandi ciphertext yang sesuai. Oleh karena itu, kedua karakter tersebut diketahui oleh penyerang dan tidak perlu ditebak. Mengapa dikatakan bahwa salt meningkatkan keamanan?

3.9 Dengan asumsi bahwa Anda telah berhasil menjawab pertanyaan sebelumnya dan memahami pentingnya garam, berikut ini adalah pertanyaan lain. Bukankah mungkin untuk menggagalkan semua pembobol kata sandi dengan secara dramatis meningkatkan ukuran salt menjadi, katakanlah, 24 atau 48 bit?

3.10 Pertimbangkan filter Bloom yang dibahas di Bagian 3.3. Tentukan k jumlah fungsi hash; N jumlah bit dalam tabel hash; dan D jumlah kata dalam kamus.

a. Tunjukkan bahwa jumlah bit yang diharapkan dalam tabel hash yang sama dengan nol dinyatakan sebagai

$$\mathbb{F} = \left(1 - \frac{k}{N}\right)^{D}$$

b. Tunjukkan bahwa probabilitas sebuah kata input, yang tidak ada di dalam kamus, akan diterima secara salah sebagai kata yang ada di dalam kamus adalah

$$P = (1 - \mathbb{F})^k$$

c. Tunjukkan bahwa ekspresi sebelumnya dapat didekati sebagai

$$P \approx (1 - e^{-kD/N})^k$$

3.11 Untuk protokol autentikasi biometrik yang diilustrasikan pada Gambar 3.12, perhatikan bahwa perangkat perekam biometrik diautentikasi dalam kasus biometrik statis namun tidak diautentikasi untuk biometrik dinamis. Jelaskan mengapa autentikasi berguna dalam kasus biometrik yang stabil tetapi tidak diperlukan dalam kasus biometrik dinamis.

3.12 Proposal autentikasi yang relatif baru adalah Secure Quick Reliable Login (SQRL) yang dijelaskan di sini: https://www.grc.com/sqrl/sqrl.htm. Tuliskan ringkasan singkat mengenai cara kerja SQRL dan tunjukkan bagaimana SQRL cocok dengan kategori jenis autentikasi pengguna yang tercantum dalam bab ini.