
Laporan Tugas Akhir
Kuliah Keamanan Sistem Informasi (EC-5010)

A Comparison
of
Proximity Authentication Approaches

Diajukan Oleh :

Lathifah Arief / 13299036



PROGRAM STUDI TEKNIK KOMPUTER
DEPARTEMEN TEKNIK ELEKTRO
FAKULTAS TEKNIK INDUSTRI
INSTITUT TEKNOLOGI BANDUNG
2004

Abstrak

Otentikasi berbasis perangkat lunak yang umum digunakan selama ini memiliki beberapa keterbatasan. Keterbatasan itu antara lain berupa aspek keamanan pasca otentikasi dan permasalahan keleluasaan jika diterapkan pada lingkungan kerja tertentu, terutama lingkungan kerja yang menggunakan sistem *pervasive computing*.

Otentikasi berbasis proksimiti menawarkan mekanisme otentikasi yang cukup aman namun lebih leluasa, yaitu dengan cara mendekat (secara fisik) kepada device tersebut. Berbagai pendekatan diupayakan untuk mencapai suatu mekanisme otentikasi berbasis proksimiti yang praktis, handal, rendah biaya dan berbagai kelebihan lainnya. Di antara pendekatan tersebut ada yang menggunakan gelombang ultrasonik, radio atau infra-red, elektromagnetik maupun optik untuk sinyal komunikasinya. Token fisik yang digunakan juga memiliki pendekatan yang beragam seperti lencana, pulpen, kartu, dan sebagainya.

Makalah ini menyajikan pembahasan penerapan otentikasi berbasis proksimiti yang telah ada serta membandingkan berbagai pendekatan yang dilakukan dalam penerapan tersebut.

Daftar Isi

Abstrak

Daftar Isi

Bab I Pendahuluan

- 1.1 Latar Belakang
- 1.2 Tujuan Penulisan
- 1.3 Batasan Masalah
- 1.4 Sistematika Penulisan

Bab II Konsep Otentikasi

- 2.1 Otentikasi Sebagai Aspek Keamanan
- 2.2 Metode Otentikasi
- 2.3 Otentikasi Berbasis Proksimiti

Bab III Berbagai Penerapan Otentikasi Berbasis Proksimiti

Bab IV Perbandingan Pendekatan Otentikasi Berbasis Proksimiti

Bab V Simpulan dan Saran

Referensi

Bab I

Pendahuluan

1.1 Latar Belakang

Maraknya komputasi dan komputersisasi di hampir semua bidang menyebabkan komputer, internet, serta layanan informasi lainnya saat ini lazim ditemukan di rumah-rumah maupun perkantoran. Orangpun kemudian lebih cenderung menyimpan informasi penting mereka di komputer daripada menyimpannya dalam bentuk berkas fisik. Adanya nilai penting yang dimiliki oleh informasi yang tersimpan pada suatu komputer menyebabkan perlunya pengamanan akses terhadap komputer dan informasi tersebut dari pihak yang tidak berhak.

Upaya pengamanan ini perlu diterapkan pada dua jalur. Jalur pertama adalah pengamanan informasi penting tersebut dari pihak yang mencoba mengaksesnya melalui jaringan. Jalur ini nantinya melibatkan perangkat keamanan jaringan seperti *firewall*, IDS (*intrusion detection system*), VPN (*virtual private network*) dan lain sebagainya. Jalur kedua adalah pengamanan informasi penting tersebut dari pihak yang mencoba mengaksesnya dari komputer atau terminal lokal. Jalur ini biasanya menggunakan mekanisme otentikasi untuk memastikan bahwa orang yang hendak mengakses komputer atau terminal tersebut adalah orang yang memang memiliki hak untuk itu.

Metode otentikasi yang paling luas digunakan untuk mengamankan akses komputer sampai saat ini adalah metode otentikasi berbasis perangkat lunak. Pada metode ini pengguna mengetikkan ID serta *password* ataupun PIN untuk dapat login dan menggunakan komputer tersebut. Metode ini mengundang permasalahan ketidak-leluasaan penggunaan jika diterapkan pada lingkungan kerja yang menyebabkan pengguna harus meninggalkan komputernya berulang kali atau pada lingkungan kerja yang menggunakan sistem *pervasive computing*. Ketidak-leluasaan ini akan sangat terasa jika, misalkan, dalam sehari pengguna harus mengetikkan ID dan *password*-nya saat login dan logout sebanyak 10 kali atau lebih.

Demi mengatasi ketidak-leluasaan ini, tidak jarang pengguna saling berbagi sesi atau menggunakan *password* yang mudah diingat sekaligus mudah pula ditebak. Lebih jauh lagi, pengguna bisa saja memilih untuk tidak logout saat harus meninggalkan komputer, yang berarti mementahkan kembali upaya pengamanan informasi yang ingin dicapai sebelumnya. Tarik ulur antara keleluasaan penggunaan dan cukupnya keamanan ini (*secure but less usable OR very usable but less secure*) membutuhkan metode otentikasi lain yang menawarkan keseimbangan antara keduanya.

Salah satu konsep otentikasi yang dinilai dapat menyeimbangkan aspek keleluasaan penggunaan dan aspek keamanan tersebut adalah konsep proksimiti. Otentikasi berbasis proksimiti dapat dipahami sebagai upaya otentikasi pengguna pada suatu perangkat cukup dengan mendekat secara fisik kepada perangkat tersebut. Saat ini ada berbagai pendekatan yang telah diupayakan untuk mencapai mekanisme otentikasi berbasis proksimiti yang praktis, handal, rendah biaya dan berbagai kelebihan lainnya.

1.2 Tujuan

Makalah ini disusun dalam upaya membuat suatu perbandingan antara berbagai pendekatan yang digunakan dalam mekanisme otentikasi berbasis proksimiti yang ada.

1.3 Batasan Masalah

Perbandingan yang akan dibahas dalam makalah ini dibatasi pada perangkat yang digunakan, kelebihan, dan kelemahan masing-masing pendekatan.

1.4 Sistematika Penulisan

Makalah ini dimulai dengan pendahuluan pada Bab 1. Bab 2 akan menyajikan secara singkat konsep otentikasi beserta beberapa metode termasuk otentikasi berbasis proksimiti, sedangkan paparan berbagai penerapan yang telah ada dapat ditemukan pada Bab 3. Bab 4 akan berisi perbandingan berbagai pendekatan otentikasi berbasis proksimiti yang telah dipaparkan sebelumnya, lalu ditutup dengan simpulan dan saran pada Bab 5.

Bab II

Konsep Otentikasi

2.1 Otentikasi Sebagai Aspek Keamanan

Otentikasi sebagai salah satu aspek keamanan dapat dimaknai sebagai metode untuk membuktikan bahwa informasi yang diakses adalah informasi yang sesungguhnya, orang yang mengakses atau memberikan informasi adalah orang yang berhak untuk hal itu, dan komputer atau server yang diakses adalah komputer atau server asli penyimpan informasi.

Dewasa ini, penggunaan komputer untuk kebutuhan pengolahan dan penyimpanan informasi sedang mengalami pergeseran relasi antara pengguna dengan komputer yang digunakan. Pergeseran ini terjadi dari paradigma *personal computing* yang menggunakan relasi *one-to-one* (seorang pengguna tertentu hanya akan bekerja dan mengakses komputer tertentu pula) ke arah paradigma *pervasive computing* yang menggunakan relasi *many-to-many* (banyak pengguna dapat menggunakan banyak komputer). Pergeseran ini terutama terjadi pada organisasi atau institusi yang menuntut fleksibilitas ataupun pergiliran dalam penggunaan komputer.

Salah satu efek dari pergeseran relasi tersebut adalah semakin menguatnya permasalahan keleluasaan penggunaan dalam penerapan otentikasi terhadap pengguna. Dalam paradigma *personal computing*, otentikasi dapat menemukan masalah keleluasaan saat diterapkan pada beberapa lingkungan kerja tertentu, misalkan lingkungan kerja rumah sakit. Permasalahan tersebut tentunya akan lebih terasa lagi pada sistem yang menerapkan *pervasive computing*, betapa sangat menyita waktu dan menyebalkan jika harus mengetikkan ID/username/ password/PIN di setiap komputer sebelum komputer tersebut dapat digunakan.

Permasalahan keleluasaan penggunaan ini seringkali melahirkan sikap ceroboh dengan meniadakan mekanisme otentikasi terhadap pengguna. Otentikasi terhadap pengguna, terlebih lagi pada pengguna yang mengakses komputer secara langsung, tidak boleh ditiadakan hanya demi keleluasaan penggunaan komputer ataupun dengan dalih bahwa pengguna adalah pihak dalam (*insider*). Banyak orang mengira bahwa ancaman keamanan terbesar berasal dari *hacker* dan virus, padahal ancaman keamanan yang paling nyata bagi suatu sistem yang terkomputerisasi justru berasal dari pihak dalam (*insider*), terutama yang memiliki hak akses secara langsung ke komputer (atau *server*). Dengan demikian, otentikasi tetap harus dipertahankan.

2.2 Metode Otentikasi

Metode otentikasi yang berkembang selama ini dapat dikategorikan menjadi dua kelompok, yaitu otentikasi berbasis perangkat lunak dan otentikasi berbasis fisik.

Metode otentikasi yang paling luas digunakan hingga saat ini adalah yang pertama, berbasis perangkat lunak. Pada metode ini pengguna mengetikkan *id/username*, *password*, PIN, pertanyaan dan jawaban rahasia atau data identitas lainnya saat login. Sistem kemudian mengacak *password* yang diberikan tadi dan membandingkannya dengan data *password* teracak yang tersimpan dalam file *password*. Jika data yang diberikan tadi cocok dengan yang tersimpan, maka pengguna akan diijinkan menggunakan komputer tersebut.

Metode ini memiliki beberapa permasalahan, antara lain :

- Pengguna memilih *password* yang gampang ditebak
- Pengguna cenderung menuliskan *password* di suatu tempat di dekat komputer
- Beberapa perangkat lunak masih menangani data proses login dalam bentuk *plaintext*
- File *password* pada beberapa sistem bisa dibaca oleh semua pengguna
- Siapapun yang secara kebetulan mengetahui informasi mengenai *id/username* dan *password* dapat login dengan berpura-pura sebagai pengguna.

Metode yang kedua, yaitu otentikasi berbasis fisik, menggunakan informasi fisik untuk otentikasi pengguna. Informasi fisik ini ada dua bentuk, yaitu informasi biometris dan perangkat fisik.

Informasi biometris merupakan ciri khas fisik (sidik jari, iris, retina, karakter suara, dll.) yang dimiliki oleh pengguna yang dapat digunakan untuk identifikasi. Untuk dapat diidentifikasi, pengguna harus hadir secara fisik pada perangkat scan. Proses identifikasi dengan informasi biometris melewati tahapan sebagai berikut :

- *scanning* : perangkat men-scan bagian fisik tertentu dari pengguna
- *feature extraction* : bagian penting dari hasil scan tadi diekstrak
- *comparison* : perbandingan data ter-ekstrak dengan data tersimpan
- *matching* : jika data ter-ekstrak cocok dengan data tersimpan, pengguna boleh lewat

Metode ini paling bagus karena pengguna tidak perlu membawa perangkat apapun dan orang lainpun sulit berpura-pura sebagai si pengguna. Namun demikian, metode ini masih cukup mahal dan belum siap untuk diterapkan secara luas.

Pada otentikasi berbasis fisik yang menggunakan perangkat fisik, perangkat akan berkomunikasi dengan komputer melalui dua cara:

- Menggunakan *scanner / reader* yang tertancap pada komputer. Setiap kali akan melakukan otentikasi, pengguna harus menggesekkan perangkat yang ada padanya ke *reader / scanner* tersebut.
- Menggunakan komunikasi tanpa kabel (*wireless*) antara perangkat yang dibawa pengguna dengan perangkat yang tertancap pada komputer. Metode otentikasi ini dalam implementasinya dikenal sebagai ‘otentikasi berbasis proksimiti’ dan perangkat yang digunakan disebut sebagai ‘perangkat proksimiti’.

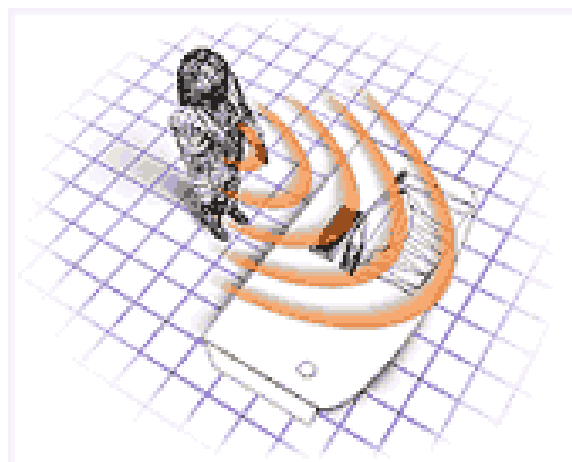
2.3 Otentikasi Berbasis Proksimiti

Inti dari konsep otentikasi berbasis proksimiti adalah memungkinkan pengguna untuk terotentikasi pada suatu perangkat cukup dengan mendekati perangkat tersebut secara fisik.

Selama ini, suatu mekanisme otentikasi dianggap “secure” jika melibatkan elemen :

- something user *knows* (mis. *password* atau pertanyaan rahasia)
- something user *has* (mis. *smartcard* atau *badge*)
- something user *is* (mis. sidik jari, iris, karakter suara).

Setiap pendekatan yang mengandalkan salah satu elemen di atas akan menemukan keterbatasan. Dua yang pertama relatif mudah diupayakan namun akan banyak bergantung pada keinginan individu pengguna untuk tidak menyebarkan apa yang mereka ‘ketahui’ dan tidak berbagi perangkat yang mereka ‘punya’. Pendekatan yang ketiga jauh lebih akurat namun menuntut biaya yang cukup besar sehingga biasanya hanya digunakan untuk kebutuhan keamanan yang tinggi. Konsep proksimiti menambahkan elemen keempat, yaitu ‘lokasi’, dalam rangka mengupayakan kondisi yang relatif lebih seimbang antara biaya, keleluasaan penggunaan dan keamanan (*usable AND sufficiently secure*).



Otentikasi berbasis proksimiti

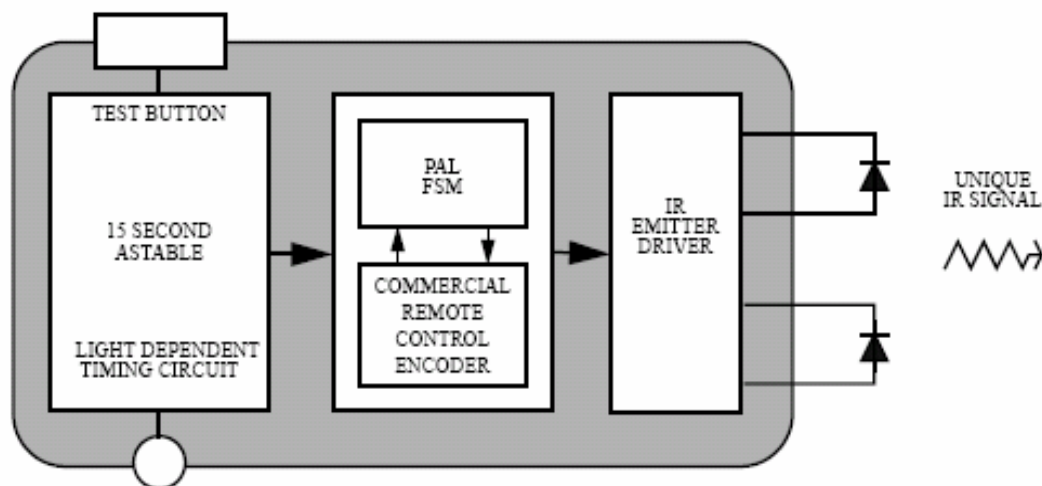
Bab III

Berbagai Penerapan Otentikasi Berbasis Proksimiti

Konsep otentikasi berbasis proksimiti sudah diterapkan dan dikembangkan oleh berbagai pihak dengan menggunakan berbagai pendekatan. Beberapa pionir penerapan konsep proksimiti di antaranya :

❖ Active Badge Location System oleh Olivetti Research Ltd. (ORL)

- Menentukan lokasi seorang staff berbekal informasi lokasi lencananya.
- ‘Active Badge’ yang digunakan oleh staff memancarkan suatu sinyal infra-red yang unik berdurasi sepersepuluh detik setiap 10 detik sekali. Sinyal periodik ini ditangkap oleh satu atau lebih sensor yang ditempatkan di sekeliling bangunan. Lokasi lencana (berarti juga lokasi staff yang mengenakannya) dapat ditentukan dari informasi mendasar yang disediakan oleh sensor.
- Lencana yang digunakan didesain dengan ukuran 55x55x7 mm dan berat 40g.



ORL ‘Active Badge’

- Suatu sinyal ‘active badge’ ditransmisikan pada sensor melalui jalur optik. Jalur ini dapat ditemukan secara tidak langsung melalui pemantulan permukaan, misalkan dari dinding. Sinyal yang digunakan antara lencana dengan sensor berupa sinyal *pulse-width modulated infrared* (IR).

Pensinyalan yang aktif dan terus menerus tentu mengonsumsi energi, sehingga laju pensinyalan menjadi isu yang penting dipertimbangkan dalam desain dan evaluasi penerapan. Dengan hanya memancarkan sinyal sekali 10 detik, konsumsi arus rata-rata dapat ditekan rendah sehingga baterai untuk lencana dapat bertahan lebih lama. Jika lencana hanya ditinggalkan di suatu tempat (misalkan pada hari libur), maka tentu lifetime efektif baterainya akan meningkat. Memberi saklar manual untuk on/off lencana oleh pengguna demi menghemat energi akan berdampak buruk jika si pengguna lupa menghidupkannya.

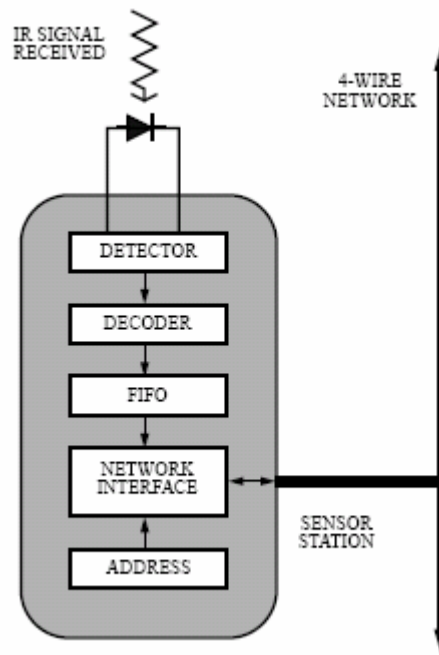
Kemungkinan dua orang yang menggunakan lencana yang berbeda berada pada satu ruangan yang sama pada satu waktu yang bersamaan bisa saja terjadi, dan ini tetap harus dapat dideteksi oleh sistem. Dengan durasi sinyal yang hanya sepersepuluh detik, maka kesempatan kedua sinyal yang dipancarkan oleh kedua lencana mengalami tumbukan hanya sekitar 2/150. Selama hanya ada sedikit orang di lokasi yang sama, maka kemungkinan mereka semua terdeteksi sekaligus tetap besar.

Pengiriman sinyal yang terputus-putus dari lencana menyebabkan lokasi lencana hanya dapat diketahui dalam jarak tempuh 15 detik (selisih waktu antar sinyal). Jika si pengguna bergerak relatif lambat, maka posisinya masih dapat ditelusuri dengan baik. Namun begitu, jika waktu 15 detik masih dapat ditoleransi dalam studi kasus pencarian staff di atas, maka untuk otentikasi berbasis proksimiti (yang ada pada permasalahan di awal makalah) tidak akan begitu disukai, karena 5 detik pun dapat membedakan antara seorang pengguna berada dalam wilayah login ataukah di wilayah logout.

Ketika digunakan untuk menjadi '*remote key*' bagi otentikasi ke suatu *secure_area* (misalkan komputer), permasalahan yang muncul dari penggunaan lencana ini adalah adanya kemungkinan sinyal yang dikomunikasinya dengan sensor direkam dan nantinya dapat di'putar ulang' untuk menghasilkan *key* yang sama. Permasalahan ini dapat dicegah dengan menggunakan suatu protokol yang merespon secara random dari sensor ke *key*.

Resiko hilang lalu dipungut oleh orang lain dapat diatasi dengan pengembangan '*Smart Badge*' yang menggunakan beberapa antisipasi untuk mengatasi permasalahan token fisik yang hilang atau tercuri. Konsepnya adalah mendesain lencana yang bisa mendeteksi momen saat lencana tersebut tidak lagi digunakan (dicopot) atau tidak dibawa (statis). Begitu lencana ini mendeteksi kedua kondisi tersebut, maka lencana tersebut mengkondisikan dirinya agar tidak bisa digunakan untuk otentikasi. Pada kenyataannya, sulit untuk menentukan seberapa cerdas suatu lencana dapat 'merasa' dan 'berfikir' bahwa ia sedang dibawa oleh penggunanya yang sah.

Salah satu isu lainnya dalam pemakaian lencana untuk otentikasi adalah posisi pemakaiannya. Orang cenderung suka memakainya di depan wilayah dada, namun ada juga yang suka meletakkannya di posisi lain, dengan alasan apapun, seperti di pinggang, atau bahkan di kaki. Sebenarnya diletakkan di manapun tidak akan jadi masalah selama lencana itu tetap dapat berkomunikasi dengan sensor.



Sensor untuk ORL 'active badge'

❖ Active Bat system oleh AT&T

- Pendekatan serupa juga dilakukan oleh AT&T untuk suatu 'Follow-me Application'
- Antarmuka pengguna dari aplikasi yang sedang digunakannya akan mengikuti si pengguna saat bergerak. Aplikasi tersebut nantinya akan ditampilkan pada display yang terdekat dengan pengguna seakan-akan diberikan oleh 'Active Bat' yang dipakai pengguna. Dengan menggunakan informasi *context_aware* pengguna serta input dari sensor, perangkat komputasi akan mengkhususkan diri untuk si pengguna.
- Pendekatan yang dipadukan disini adalah penggunaan alat tertentu sebagai key untuk berkomunikasi dengan sensor untuk menentukan lokasi pengguna (*location based context aware system*) dengan penyimpanan informasi atas apa yang sedang dilakukan si pengguna (*action based system*).

❖ ComputerProx™ TF2000 oleh ComputerProx Corp.

Suatu komputer yang dilengkapi dengan peralatan ComputerProx™ TF2000 akan secara otomatis ‘merasakan’ saat seorang pengguna mendekat. ComputerProx™ TF2000 akan mengotentikasi pengguna dengan menggunakan metode yang telah dipilih oleh pengguna sebelumnya (password, biometris, smart card, token, dsb).



ComputerProx™ TF2000

TF2000 juga menggunakan ultrasonik untuk mendeteksi keberadaan seseorang. Saat pengguna menjauh meninggalkan jarak tertentu dari PC, sensor sonar ultrasonik yang ada pada ComputerProx™ TF2000 akan mengirim perintah yang sama seperti yang digunakan pengguna secara manual pada PC (mis. Ctrl-Alt-Del pada Windows 2000) untuk menutup sesi si pengguna dan kembali ke mode login.

Perintah-perintah dikomunikasikan dengan PC tanpa butuh *driver* khusus. TF2000 terhubung ke PC melalui *port* USB dan dikonfigurasi melalui *keyboard*. Pemrograman *keystroke sequence*, *timeout*, serta beragam opsi lainnya tersimpan dalam suatu memori *non-volatile* yang *onboard*.

Selama ketiadaan pengguna, komputer dapat diset agar berada dalam mode stand-by sehingga lebih menghemat energi.

Spesifikasi :

- Rentang jarak pembacaan minimum 14 inchi (35,54cm) dan maksimum yang direkomendasikan 42 inchi (106,7cm), namun masih memiliki batas toleransi hingga 60 inchi (152,4cm).

Dimensi :

- **Reader** : 1.78” x 1.98” x 0.84” (4,52 cm x 5,03 cm x 2,13 cm)

- Kabel: 72” (182,88 cm) USB

Power Supply :

- 5.0 V via Port USB

Data :

- Port USB

Lingkungan Operasi :

- Temperatur 5 – 55 C
- Kelembaban 0-95% kelembaban relatif (*non-condensing*)

Transducer :

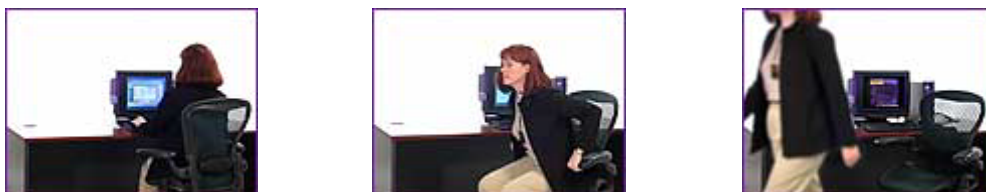
- Frekuensi 40KHz

Minimum PC Requirement :

- Windows 98se, ME, 2000 atau XP.
- Port USB
- CD-ROM drive
- 200K space kosong pada disk

❖ **XyLoc oleh Ensure Tech.**

Xyloc menawarkan solusi keamanan yang tetap melindungi jaringan setelah seorang pengguna login. Xyloc terdiri atas suatu pemancar gelombang radio tanpa kabel (“Key”) yang dibawa oleh pengguna dan suatu penerima gelombang radio (“Lock”) yg menancap pada komputer dan. Untuk menentukan identitas serta lokasi si pengguna relatif terhadap komputer, Lock dan Key harus tetap dalam komunikasi radio konstan sampai berjarak 15 meter.



Pengguna meninggalkan workstation

Saat seorang pengguna yang mengenakan XyLoc Key mendekati suatu komputer yang dilindungi oleh XyLoc, Key secara otomatis akan mentransmisikan suatu kode ID 32-bit yang unik dan terenkripsi kepada Lock. Lock akan melakukan verifikasi identitas pengguna. Jika sah, maka Xyloc akan melepaskan penguncian yang sebelumnya berlaku pada *keyboard*

dan layar monitor. Sedangkan jika tidak sah, maka sistem akan tetap terkunci dan informasi di dalamnya tetap aman.

XyLoc menyediakan fleksibilitas bagi pengguna baik untuk login otomatis dengan fitur hands-free maupun untuk secara manual memilih nama dan memasukkan password pada situasi lain yang menuntut begitu. XyLoc juga dapat diintegrasikan dengan penghitungan keamanan lainnya mulai dari token sampai biometris.

XyLoc menyediakan *override password* agar pengguna tetap dapat mengakses *workstation* mereka jika lupa membawa Key. Saat *override password* dimasukkan, maka perangkat lunak XyLoc akan mengirimkan informasi kejadian ini pada administrator.

XyLoc memiliki mekanisme enkripsi pada *password* dan juga file *password* untuk mencegah akses yang tidak sah terhadap file data yang terdapat pada harddrive suatu PC desktop ataupun notebook yang dilindungi oleh XyLoc tersebut.

Persyaratan pada XyLoc Client

- Microsoft Windows 98, NT 4.0 dengan SP 5, 2000, XP atau XPe
- CD-ROM drive atau koneksi jaringan pada server yang menjalankan XSS
- USB port
- 5 MB space pada hard disk.

Persyaratan pada XyLoc Security Server

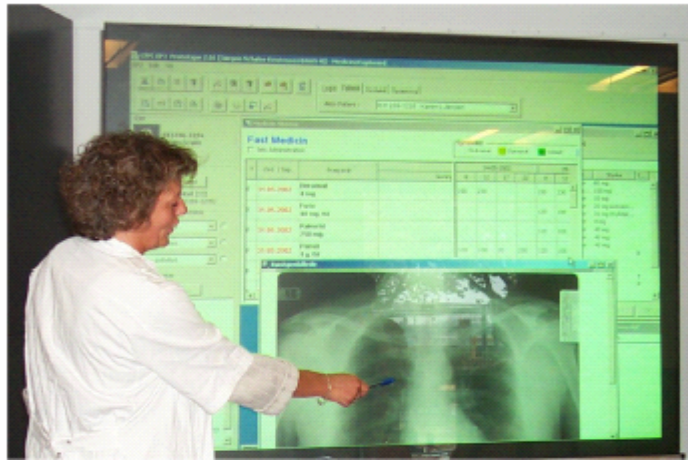
- PIII 1GHz, memori 256 MB, dan 2GB space pada disk serta alamat IP statis
- Windows NT 4.0 Server dengan Option Pack 4 atau lebih, atau Windows 2000 Server
- Internet Information Services (IIS) 4.0 atau yang lebih, terinstal dan beroperasi

Supported Environment lainnya:

- Citrix MetaFrame
- Microsoft Active Directory 2000 atau 2003
- Microsoft Terminal Services
- Novell eDirectory/NMAS

Lock dan *Key* pada XyLoc menggunakan gelombang radio 300, 800 atau 900 MHz, tergantung pada negara tempatnya terinstal.

❖ Context-Aware User Authentication oleh Center for Pervasive Computing



Akses terhadap well-based display pada suatu konferensi

Pada gambar di atas terlihat penggunaan *Personal Pen* untuk otentikasi pengguna ke komputer. Suatu 'active badge' tersemat di bajunya (tidak terlihat) tetap diperlukan untuk sistem context-aware terhadap lokasinya.

Penerapan kali ini bertujuan membangun sistem *pervasive computing* dengan memanfaatkan otentikasi berbasis proksimiti. Persyaratan untuk mekanisme otentikasi pengguna pada sistem *pervasive computing* :

- ❖ *Proximity Based* → *If I use a computer, it should know me automatically*
- ❖ *Secure* → *data is very sensitive!*
- ❖ *Active Gesture* → *pick the right machine in the room!*

Ada 3 prinsip utama dalam otentikasi berbasis proksimiti pada sistem *context-aware* :

- Menggunakan token fisik untuk *active gesturing* dan as the basis kriptografis untuk otentikasi. Token fisik yang digunakan disini adalah *smart card*.
- Menggunakan sistem *context-awareness* untuk verifikasi lokasi si pengguna dan untuk otomatis logout jika pengguna menjauh dari computer pada jarak tertentu.
- memiliki mekanisme '*fall-back*', sehingga jika salah satu komponen di atas gagal, maka mekanisme otentikasi akan otomatis switch pada mekanisme otentikasi tradisional atau mekanisme biometris.

Token Fisik

Berbagai pendekatan token (selain lencana dan *personal pen*) juga ditemukan pada beberapa penerapan :

- HID brand reader oleh BlueBoard project IBM
- RFID tag oleh AwareHome at Georgia Tech
- RFID card oleh FX PAL; the Personal Interaction Points (PIPs) System

Otentikasi Menggunakan Kartu

- Otentikasi dengan kartu sebagai token fisik bukan hanya lebih murah daripada teknologi biometris namun juga bisa melengkapi keberadaannya, menambahkan fitur dan aplikasi yang lebih terjangkau.
- Kartu dapat digunakan sebagai secondary credential dalam implementasi kontrol akses sehingga selain informasi biometris yang dimilikinya seorang pengguna juga harus memiliki kartu untuk mendapatkan akses.
- Kartu juga bisa digunakan untuk menyimpan template biometris yang memungkinkan identitas pengguna diperiksa pada suatu sistem yang kompatibel lainnya yang tidak bisa melibatkan langsung si pengguna.
- Beberapa keuntungan otentikasi menggunakan kartu
 - *Cost effective*
 - Relatif lebih aman daripada ID & *password*
 - Memperluas aplikasi untuk teknologi biometris
 - Pemusatan berbagai solusi keamanan

Teknologi otentikasi menggunakan kartu punya 2 kelompok dasar : **Proximity Cards**, dan **i-CLASS Card** (turunan dari smartcard).

Proximity Card

Suatu sinyal magnetic diinduksikan ke suatu coil dan dimasukkan dalam kartu. Sinyal ini akan mentransmisikan card number ke reader untuk diotentifikasi Proximity Card aslinya digunakan untuk operasi *hands free*, pengguna tidak perlu meletakkan atau menggesekkan kartu tersebut ke reader manapun. Rentang jarak pembacaan merupakan isu penting. Jaminan ketepatan pembacaan pun menjadi isu selanjutnya saat lebih dari satu pengguna melewati suatu reader bersamaan. Batasan rentang pembacaan terdapat pada *passive cards*, terutama jika masalah ketebalan kartu terasa mengganggu, karena kartu yang memiliki rentang

pembacaan yang lebih panjang biasanya mempunyai tampilan fisik yang lebih tebal. Proses manufaktur menyebabkan proximity card menjadi lebih mahal.



Proximity Card

Smart Card & iCLASS smart card

Mirip dengan kartu kredit plastik yang banyak beredar saat ini, *smartcard* memiliki embedded microprosesor atau memori di dalamnya. Ada dua jenis smartcard: *memory* dan *microprocessor*. *MemoryCard* hanya menyimpan data dengan security sebagai opsi. *MicroprocessorCard*, dapat menambah, menghapus dan memodifikasi informasi dalam card tersebut, memiliki sejenis sistem operasi, port input/output dan memiliki fitur *security*.

Dalam teknologi kartu, iClass aslinya tergolong dalam platform SmartCard yang menawarkan *contact free*, memungkinkan penyimpanan *template* biometris pada *card*, *user-friendly*, meyakinkan, nyaman digunakan, biayanya terjangkau dan handal untuk teknologi otentikasi berbasis proksimiti dengan HID. iCLASS card berikut reader-nya menawarkan fitur unik yang lebih maju dari teknologi *radio frequency identification* (RFID) tradisional lainnya. Fitur tersebut berupa :

- Otentikasi yang mutual
- *Pembacaan dan penulisan data yang 'secure'*
- *Cryptographic data storage*
- *User definable access keys*

Seluruh transmisi data dengan frekuensi radio antara card dengan reader dienkripsi. Dengan menggunakan teknik enkripsi berstandar industri, iCLASS mereduksi resiko terhadap data maupun kartu (duplikasi *card*).

BAB IV

Perbandingan Pendekatan Otentikasi Berbasis Proksimiti

Selain menggunakan *infra-red* untuk komunikasi antara ‘Key’ dan ‘Lock’, gelombang elektromagnetik juga dapat digunakan untuk menentukan lokasi serta orientasi gerak pengguna dengan resolusi dan akurasi yang lebih tinggi. Namun demikian, kelemahannya adalah mahal dan membutuhkan kesabaran untuk mengontrolnya. Selain itu pelacak elektromagnetik hanya mampu menjangkau rentang jarak yang pendek (beberapa meter) dan sensitif terhadap keberadaan objek metal.

Pelacak optik juga sangat handal, dapat mencapai akurasi serta resolusi yang mirip dengan penggunaan elektromagnetik. Namun, selain mahal juga bekerja pada lingkungan kerja terbatas serta cenderung rumit. Contoh penggunaannya adalah *laser-scanning system* untuk melacak gerak tubuh manusia.

Sistem penentuan posisi berbasis gelombang radio seperti *Global Positioning System* (GPS) and LORAN sangat sukses di berbagai area aplikasi tapi tidak cukup efektif jika digunakan dalam bangunan dikarenakan pantulan sinyal radio yang sering terjadi dalam lingkungan *indoor*. Sistem penentuan posisi berbasis gelombang radio seperti XyLoc tentu banyak, tapi hanya menawarkan informasi lokasi dengan akurasi sekitar 50 cm dan masih mungkin untuk mengalami interferensi.

Informasi lokasi pengguna juga dapat diturunkan dari analisis data video seperti yang diterapkan oleh *MIT Smart Rooms project*, namun ini membutuhkan terlalu banyak proses komputasi.

Kelebihan sinyal *infra-red* (IR) untuk pensinyalan antara *key* yang ada pada pengguna dengan sensor yang diletakkan pada atau di sekitar komputer terutama karena IR :

- *solid-state emitter* serta detektornya dapat dibuat sangat kecil dan murah (tidak seperti *ultrasonic transducers*)
- dapat beroperasi hingga rentang 6 m
- sinyalnya dipantulkan oleh sekat sehingga tidak bersifat *directional* saat digunakan dalam ruang sempit
- tidak menembus dinding, tidak seperti sinyal radio yang dapat menyusup saat menemukan sekat pada bangunan

- komunikasi infrared juga digunakan secara luas dalam aplikasi yang beragam, termasuk sebagai basis bagi wireless LAN.
- Teknologi IR telah dieksploitasi secara komersil sehingga relatif tidak mahal dan siap untuk digunakan pada pengembangan aplikasi baru, termasuk aplikasi Active badge.

Solusi optimal berikutnya selain *infra-red* adalah penggunaan ultrasonik untuk penentuan lokasi. Pengukuran dilakukan terhadap waktu yang dibutuhkan oleh pulsa suara dari suatu pemancar ultrasonik menuju penerimanya. Jarak antara pemancar dan penerima dapat dihitung dari informasi waktu transmisi, sehingga lokasi pemancar yang seharusnya juga merupakan lokasi pengguna, dapat ditentukan.

Dari sekian pendekatan token fisik, bentuk kartu masih menjadi raja. Adapun di antara jenis kartu yang dapat digunakan, *smartcard* (beserta turunannya) masih merupakan pilihan yang paling optimum. Beberapa kelebihan penggunaan *smartcard* sebagai token fisik dibanding token fisik lainnya adalah :

- *Tamper-resistant*
- Informasi yang tersimpan di dalamnya bisa berupa kode PIN code dan read-write protected
- Mendukung enkripsi
- Setiap *smartcard* punya serial number yang unik
- Selain penyimpanan, juga memungkinkan pemrosesan informasi
- Dapat berkomunikasi dengan perangkat komputasi melalui *smartcard reader* yang sudah banyak dikembangkan
- Informasi dan aplikasinya dapat diupdate tanpa harus membuat kartu baru
- *Portable, easy to use & familiar* bagi pengguna

BAB V

Simpulan dan Saran

Masih dimungkinkan bagi pihak asing untuk menyusup sebagai pengguna dengan melakukan beberapa hal sebagai berikut:

1. Mencuri token dan menyusup ke lokasi komputer pengguna yang sah
 - (a) Menjawab verifikasi lokasi dengan token penentu lokasi
 - (b) Melakukan trik pada bagian lain dari sistem lokasi
2. Mencuri token dan ada di ruangan yang sama dengan pengguna yang sah.
3. Mencuri token dan mengetahui juga *override password* milik pengguna yang sah.
4. Melakukan serangan terhadap proxy.

Untuk pensinyalan, opsi yang paling optimal adalah *infrared* dan ultrasonik. Sedangkan untuk token fisik, *smartcard* masih merupakan opsi terbaik.

Perlu dilakukan pengujian lebih lanjut terhadap berbagai pendekatan yang telah ada serta pengembangan untuk mendapatkan pendekatan yang lain, baik untuk pensinyalan maupun token fisik.

Referensi :

- [1] <http://www.sans.org/rr/papers/index.php?id=102>
- [2] <http://ciae.cs.uiuc.edu/SRG/context-aware-auth.pdf>
- [3] <http://ww.computerprox.com>
- [4] <http://www.ensuretech.com/products/technology/technology.html#HowXyLocWorks>
- [5] http://www.hrsLtd.com/identification_technology/card_authentication.htm
- [6] [http://www.cs.colorado.edu/~rhan/CSCI_7143_002_Fall_2001/Papers/Want92_ActiveB
adge.pdf](http://www.cs.colorado.edu/~rhan/CSCI_7143_002_Fall_2001/Papers/Want92_ActiveB
adge.pdf)
- [7] <http://www-2.cs.cmu.edu/~15-821/CDROM/PAPERS/ward97.pdf>