AUREN: Sistem Pengamanan *Smartphone* dengan Penghapusan Informasi Berharga dan Pengiriman Informasi untuk Pelacakan Otomatis

Narenda Wicaksono

Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132
e-mail : if12023@students.if.itb.ac.id

ABSTRAK

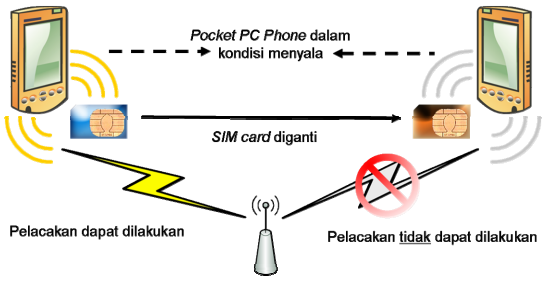
Makalah ini akan menjelaskan tentang pengembangan aplikasi yang menerapkan metode proteksi terhadap informasi berharga yang terdapat di dalam *smartphone* dengan melakukan penghapusan secara otomatis terhadap informasi tersebut. Aplikasi yang diberi nama AUREN ini juga menerapkan metode pengiriman informasi yang dapat digunakan untuk membantu pelacakan keberadaan dari *smartphone* yang dicuri ke nomor telepon yang sudah didefinisikan sebelumnya secara otomatis. Latar belakang dari pengembangan aplikasi ini karena *smartphone* adalah piranti genggam yang memiliki fungsionalitas yang lengkap. Hal tersebut menyebabkan *smartphone* menjadi sebuah piranti yang berharga dan rawan dicuri. Mengingat piranti *smartphone* sering digunakan untuk menyimpan informasi berharga pemiliknya, maka proteksi terhadap informasi berharga yang dimiliki oleh sebuah *smartphone* menjadi sesuatu hal yang penting. AUREN adalah aplikasi yang diimplementasikan secara khusus untuk *smartphone* dengan sistem operasi *Windows Mobile 2003 Pocket PC Phone Edition*. AUREN dibangun dengan menggunakan bahasa pemrograman C# dan memanfaatkan *platform .NET Compact Framework*.

Kata kunci: proteksi, *smartphone*, hilang, *SIM card*, diganti

Makalah diterima 2 Februari 2007. Revisi akhir 1 Februari 2007.

1. PENDAHULUAN

Saat ini *smartphone* banyak memberikan keuntungan bagi perusahaan. Piranti *smartphone*, seperti *Pocket PC Phone* dapat meningkatkan kinerja profesional perusahaan karena fungsionalitasnya sebagai telepon genggam, dan komputer genggam sekaligus. Dengan bentuk yang kompak dan fungsionalitas yang lengkap, *smartphone* menjadi sebuah piranti komunikasi yang bernilai, berharga tinggi, dan rawan dicuri. Berdasarkan *Pointsec Mobile Usage Survey*, 22% pemilik *smartphone* di dunia ini kehilangan pirantinya [1]. Berbagai masalah akan timbul bila sebuah *smartphone* hilang dicuri. Oleh karena itu proteksi terhadap informasi dalam *smartphone* menjadi mutlak diperlukan. Selain itu jika ingin dilakukan pelacakan terhadap keberadaan piranti yang hilang, maka pelacakan hanya dapat dilakukan jika *SIM card* belum diganti dan *smartphone* masih berada dalam kondisi menyala [2] seperti dideskripsikan oleh gambar 1 berikut ini.



Gambar 1 Pelacakan *Smartphone* Tergantung SIM Card

Berdasarkan penjelasan tersebut, terdapat dua permasalahan. Permasalahan yang pertama adalah jika sebuah *smartphone* yang mengandung informasi berharga dicuri, proteksi apa yang bisa dilakukan terhadap informasi berharga tersebut? Proteksi yang dapat dilakukan adalah dengan mematikan *visibility* terhadap informasi tersebut atau melakukan penghapusan secara otomatis (*self destruction*). Permasalahan yang kedua adalah jika *SIM card* telah diganti, masih mungkinkah pelacakan terhadap sebuah *smartphone* dilakukan? Hal yang bisa dilakukan adalah dengan memasang sebuah aplikasi dalam *smartphone* yang dapat secara otomatis mengirimkan informasi dari *smartphone* tersebut ke nomor tertentu secara periodik. Aplikasi tersebut diberi nama AUREN.

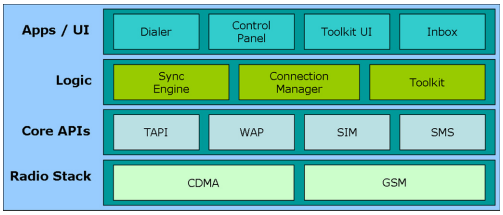
2. SISTEM KOMPUTASI *MOBILE*

Piranti yang mendukung komputasi *mobile* semakin banyak digunakan oleh masyarakat. Secara definisi komputasi *mobile* adalah sebuah aktivitas melakukan proses komputasi dengan menggunakan piranti yang memanfaatkan jaringan namun secara fisik tidak tersambung kabel (*wireless*) [3]. Suatu hal yang harus diperhatikan dari sebuah piranti yang memiliki kemampuan untuk melakukan proses komputasi secara *mobile* adalah piranti tersebut memiliki sumber daya yang terbatas bila dibandingkan dengan piranti konvensional [4]. Dampak dari sumber daya yang terbatas menyebabkan segala sesuatu yang tersimpan dalam memori harus mangkus dan sangkil. Sedangkan tantangan yang muncul dari pengembangan sistem komputasi *mobile* adalah manajemen sumber daya dan konsistensi konektivitas data. Sumber daya seperti daya, *bandwith*, atau memori yang tersedia dalam

piranti terbatas. Oleh karena itu pemanfaatannya harus dihemat dengan meminimalisasi penggunaaan *thread* yang tidak perlu.

3. *SMARTPHONE*

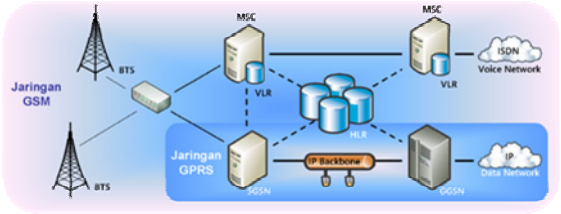
Smartphone adalah sebuah piranti yang mengintegrasikan fungsi dari telepon genggam, *Personal Digital Assistant* (PDA) dan fungsi lainnya [5]. Semua perangkat telepon genggam yang memiliki fungsionalitas PDA, misalnya *Pocket PC Phone* dapat dikategorikan sebagai *smartphone*. Sebuah piranti *smartphone* selalu dilengkapi dengan sebuah sistem operasi yang spesifik piranti. Sistem operasi *smartphone* yang saat ini beredar antara lain adalah Windows Mobile 2003. Arsitektur sistem operasi *Windows Mobile 2003* terdiri dari empat *layer* (lapisan) [6], yaitu: aplikasi/UI (*User Interface*), *logic*, *core* API (*Application Programming Interface*), dan *Radio Stack*. Aplikasi dapat mengakses fitur piranti dengan memanfaatkan API yang disediakan oleh sistem operasi. Lihat gambar 2. *Windows Mobile 2003* juga mendukung penggunaan beberapa algoritma hash kriptografi, antara lain: MD2, MD4, dan MD5.



Gambar 2 – Arsitektur Sistem Operasi *Smartphone*

Smartphone dapat berfungsi sebagai telepon genggam. Seperti layaknya sebuah piranti telepon genggam, sebuah *smartphone* memiliki identitas piranti berupa IMEI (International Mobile Equipment Identity) [7]. Selain itu *smartphone* juga memanfaatkan jaringan telepon genggam seperti GSM atau CDMA. Oleh karena itu sebuah *smartphone* harus dilengkapi dengan sebuah SIM (Subscriber Identity Module) card sebagai identitas piranti di jaringan [6].

4. *GLOBAL SYSTEM FOR MOBILE* (GSM)



Gambar 3 - Arsitektur Jaringan GSM-GPRS

Pada dasarnya, teknologi GSM memiliki dua komponen utama, yaitu: jaringan GSM dan *Mobile System*. *Mobile System* terhubung dengan *GSM Network* yang kemudian akan menghubungkan *Mobile System* tersebut dengan *World Network*. *World Network* dapat terdiri dari *Voice* (ISDN) *Network* dan atau *Data Network* [8]. Arsitektur dari GSM dapat dilihat pada gambar 3.

Perangkat genggam GSM menjadi suatu perangkat yang rawan dicuri. Untuk memerangi hal tersebut, setiap perangkat genggam dilengkapi dengan nomor IMEI (*International Mobile Equipment Identity*). IMEI adalah identitas dari sebuah perangkat genggam yang tersimpan dalam perangkat genggam tersebut.

Selain IMEI, untuk memerangi masalah pencurian perangkat genggam, dalam arsitektur GSM terdapat basis data yang disebut dengan *Equipment Identity Register* (EIR). Dalam EIR tersimpan:

1. *White list*, yaitu daftar perangkat genggam yang valid.
2. *Black list*, yaitu daftar perangkat genggam yang memiliki IMEI tidak valid karena dilaporkan dicuri.
3. *Gray list*, yaitu daftar perangkat genggam yang sedang dilacak.

Dengan terdaftarnya perangkat genggam yang tidak valid dalam EIR, maka pelacakan terhadap perangkat genggam yang hilang secara teoritis dapat dilakukan dengan melacak data dari *SIM card* yang terdapat pada perangkat genggam tersebut. Akan tetapi beberapa operator jaringan GSM sengaja tidak melengkapi jaringan mereka dengan EIR karena alasan biaya. Tidak ada data resmi mengenai apakah operator jaringan GSM di Indonesia melengkapi sistem jaringan GSM mereka dengan EIR. Tetapi yang pasti adalah tidak ada operator jaringan GSM di Indonesia yang memberikan layanan untuk pelaporan pencurian perangkat genggam.

5. METODE PROTEKSI YANG DIUSULKAN

Saat pertama kali digunakan, pemilik *smartphone* diharuskan untuk mengisikan *password*. Kemudian pemilik akan diminta untuk memasukkan nama pemilik, nomor telepon yang akan dihubungi jika *smartphone* hilang, dan daftar *file/folder* yang akan dihapus jika *smartphone* hilang. Bila *smartphone* dicuri dan setelah itu *SIM card* diganti maka hal yang akan dilakukan oleh aplikasi adalah:

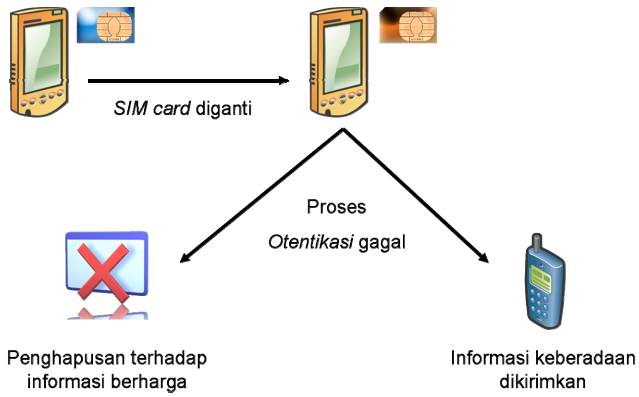
1. Antarmuka otentikasi akan muncul.
   Proses otentikasi dilakukan dengan meminta pengguna untuk memasukkan *password* dalam 60 (enam puluh) detik dengan lima kali kesempatan memasukkan *password*.
2. Jika pengguna gagal memasukkan *password* yang valid.
   Password yang valid gagal dimasukkan dalam waktu kurang dari enam puluh detik atau lima kali

kesempatan, maka aplikasi akan melakukan tiga hal utama, yaitu:

a. Melakukan penghapusan terhadap *file/folder* yang mengandung informasi berharga. Daftar *file/folder* ini harus didefinisikan terlebih dahulu oleh pemilik informasi berharga.
b. Mengirimkan informasi yang dapat digunakan untuk melacak keberadaaan dari *smartphone*. Informasi yang dikirimkan antara lain: IMEI, nama pemilik yang legal, daftar panggilan yang masuk atau keluar dan daftar buku telepon yang terdapat pada *SIM card* pengguna ilegal. Jenis dan daftar dari informasi yang dikirimkan akan dibahas pada sub bab 5.1.
c. Menjadi *invisible*. Sementara informasi-informasi tersebut dikirimkan, *smartphone* tetap dapat digunakan dengan normal sehingga tidak menimbulkan kecurigaan penggunanya. Strategi ini akan dibahas pada sub bab 5.2.

3. Jika pengguna berhasil memasukkan *password* yang valid maka aplikasi akan langsung mati.

Perilaku tersebut dideskripsikan dalam Gambar 4.



Gambar 4 Identifikasi Perilaku Aplikasi yang Diharapkan

5.1. Informasi yang Dikirimkan

Informasi yang dikirimkan oleh aplikasi adalah informasi yang dapat digunakan untuk membantu pelacakan keberadaan dari *smartphone* yang hilang dicuri. Informasi yang dikirimkan ke nomor yang telah didefinisikan adalah:

1. SMS pertama yang akan dikirimkan berisi informasi tentang nama pemilik yang legal, jenis *smartphone*, dan nomor IMEI.
2. SMS kedua yang dikirimkan adalah daftar buku telepon yang terdapat pada *SIM card*. Daftar ini akan dikirimkan secara parsial per SMS dengan periode waktu tertentu. Setiap SMS minimal akan berisi tujuh kontak telepon. Setiap kontak berisi nama dan nomor telepon.
3. SMS ketiga yang akan dikirimkan adalah daftar panggilan terakhir yang dilakukan oleh pengguna ilegal. SMS yang ketiga ini akan dikirimkan secara periodik. Dengan rentang waktu tertentu. Daftar panggilan terakhir yang dikirimkan adalah semua jenis panggilan: panggilan masuk, panggilan keluar, dan panggilan tak terjawab. Setiap panggilan dikirimkan dengan format: nama dan nomor telepon.

Semua informasi tersebut hanya dikirimkan melalui SMS jika syarat yang dibutuhkan untuk mengirimkan SMS terpenuhi. Syarat yang harus dipenuhi untuk mengirimkan sebuah SMS adalah keberadaan sinyal jaringan GSM dan pulsa yang cukup untuk mengirimkan SMS. Jika syarat tersebut tidak terpenuhi, maka proses pengiriman akan menunggu hingga kondisi tersebut terpenuhi. Jika SMS yang berisi informasi yang dapat digunakan untuk melacak keberadaan dari *smartphone* gagal terkirim, maka proses pengiriman akan terus dicoba hingga dipastikan informasi tersebut terkirim.

5.2. Penggunaan Sumber Daya

Pada saat *run-time,* aplikasi yang kelak akan dikembangkan harus menggunakan sumber daya seminimal mungkin agar tidak menimbulkan kecurigaan pemakainya. Hal ini dikarenakan sumber daya yang dimiliki oleh sebuah *smartphone* sangat terbatas. Jika aplikasi menggunakan sumber daya yang terlalu banyak, maka proses lain yang berjalan akan terhambat dan akan menimbulkan kecurigaan pengguna ilegal bahwa ada sebuah aplikasi yang berjalan. Seperti yang telah dijelaskan pada Sub Bab 2.3.2.1, cara yang dapat dilakukan untuk mengatasi hal ini ada dua, yaitu: meminimalisasi penggunaan kode dan *thread.*

5.3. Penyimpanan *Password*

Menyimpan informasi penting seperti *password* pada *key registry* ternyata bukan merupakan pilihan terbaik, karena *password* tersebut dapat dengan mudah dibuka dengan aplikasi seperti *PHM Registry Editor*. Walaupun *password* tersebut dienkripsi, akan tetapi *password* tersebut dapat diubah nilainya, karena *registry editor* memungkinkan hal tersebut. Oleh karena itu *password* akan disimpan dalam suatu *file* tersembunyi yang dienkripsi. Keputusan ini diambil karena berbagai alasan antara lain:

1. Aplikasi *File Explorer* milik sistem operasi *Windows Mobile* tidak memiliki fitur yang dapat mengeksplorasi *hidden file.*
2. Bila terjadi suatu kondisi dimana *file password* ditemukan maka perubahan terhadap *file* tersebut tidak dapat dilakukan. Aksi yang dapat dilakukan hanya penghapusan terhadap *file* tersebut.

Password akan diubah menjadi *hash code* dengan fungsi MD5. Setelah itu *file password* akan dienkripsi

dengan algoritma enkripsi TripleDES. Algoritma enkripsi ini dipilih karena selain cukup kuat, juga didukung oleh *CryptoAPI Windows Mobile*. Sehingga penggunaan algoritma ini akan mengefisiensikan penggunaan kode, karena tidak perlu menuliskan algoritma enkripsi lagi dalam kode program. Setelah itu *file password* akan disembunyikan dalam suatu lokasi tertentu.

6. *APPLICATION PROGRAMMING INTERFACE*

AUREN akan mengakses fitur piranti dengan memanfaatkan API yang disediakan oleh sistem operasi *Windows Mobile 2003*. API yang akan digunakan adalah SIM API, SMS API, Phone API dan *CE Messaging* API (CEMAPI). Pengaksesan fitur piranti yang memanfaatkan API antara lain digunakan untuk:

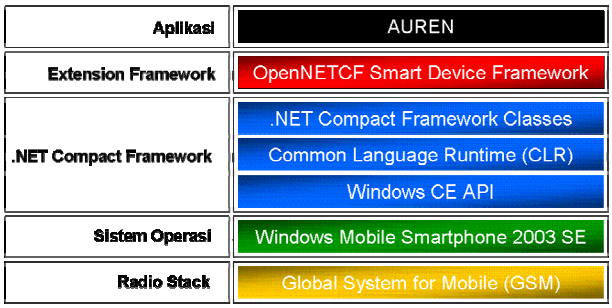
1. Mengirimkan pesan.
   Method SmsGetPhoneNumber dan *SmsSendMessage* dari SMS API akan digunakan masing-masing untuk mendapatkan nomor aktual dari *SIM card* yang digunakan dan mengirimkan pesan SMS. Sedangkan untuk mendapatkan nomor telepon dari SMS storage, digunakan interface IMailRuleClient, IMsgStore, dan IMessage dari CEMAPI.
2. Membaca daftar nomor telepon dari *SIM card.*
   AUREN akan memanfaatkan *method SimReadPhonebookEntry* dari *SIM* API untuk membaca daftar nomor telepon yang tersimpan dalam *SIM card*.
3. Membaca daftar panggilan terakhir (*call log*).
   Untuk mendapatkan daftar panggilan telepon, digunakan *method PhoneGetCallLogEntry* dari Phone API.

Penggunaan *API Smartphone* dikonstruksikan melalui C++. Pengaksesan API menjadi tidak mudah karena bahasa pemrograman yang digunakan dalam pengembangan AUREN adalah C#. Hal ini dikarenakan kelakuan API tidak dapat dikontrol secara penuh oleh aplikasi. *Method* dari API *smartphone* yang disebut *unmanaged code* dikendalikan oleh aplikasi *managed code*. Untuk menjembatani penggunaan *unmanaged code* oleh *managed code* dibutuhkan teknik yang disebut *marshalling*. Teknik ini menggunakan *method static* dari *kelas marshall* yang disediakan oleh *platform* .NET.

7. ARSITEKTUR AUREN

Arsitektur dari AUREN digambarkan pada Gambar 5. Dari Gambar 5, dapat dilihat bahwa AUREN tersusun atas beberapa komponen. Berikut penjelasan untuk setiap komponen :

1. Komponen *Radio Stack* yang digunakan adalah GSM. Komponen ini dimanfaatkan oleh AUREN untuk mengirimkan pesan SMS.
2. Komponen Sistem Operasi yang akan dimanfaatkan fungsionalitasnya oleh AUREN adalah *Windows Mobile Smartphone 2003 Second Edition*.
3. Komponen *.NET Compact Framework* menyediakan API untuk AUREN. Komponen ini juga akan memanfaatkan API *smartphone.* Komponen *Extension Framework* berupa *framework* tambahan yang bekerja diatas *.NET Compact Framework*. Untuk mengembangkan aplikasi AUREN, digunakan *framework "OpenNetCF"* yang menyederhanakan penggunaan API *smartphone*.



Gambar 5 Arsitektur AUREN

8. KESIMPULAN

Telah berhasil dikembangkan sistem keamanan *smartphone* dengan proteksi informasi berharga. Sistem ini dapat melindungi informasi-informasi penting yang mungkin dapat disalahgunakan jika sampai jatuh ke tangan orang yang tidak tepat. Metode penghapusan memang bukan merupakan metode yang terbaik, akan tetapi *smartphone* memiliki limitasi dalam pemrosesan data. Sehingga proses enkripsi membutuhkan waktu yang tidak sedikit, terutama jika data yang dienkrip berukuran besar. Oleh karena itu metode ini dapat dikatakan yang terbaik untuk piranti *mobile*. Selain itu telah berhasil dikembangkan sistem keamanan *smartphone* yang mampu melakukan mengirimkan pengiriman bukti elektronik secara otomatis. Kemampuan ini dapat menjawab masalah pencurian *smartphone* di dunia dan di Indonesia. Bila menjadikan perangkat hukum di Indonesia sebagai acuan, maka aplikasi AUREN merupakan sebuah aplikasi yang dapat memudahkan proses hukum terutama untuk membantu pelacakan *smartphone* yang hilang dicuri. Pembahasan mengenai fungsionalitas AUREN dalam pelacakan *smartphone* yang hilang dicuri terkait dengan perangkat hukum di Indonesia dideskripsikan di [8].

Metode ini proteksi otomatis ini untuk kedepannya cukup potensial untuk dikembangkan pada *smartphone* dengan *platform* selain *Windows Mobile*. Mengingat pasar *smartphone* saat ini tidak hanya dikuasai oleh *smartphone* yang menggunakan *platform Windows Mobile*. Selain itu pengembangan AUREN tidak terbatas hanya untuk *smartphone* saja, metode ini dapat pula diterapkan untuk *handphone* konvensional.

9. DAFTAR REFERENSI

[1] Fogie, Seth. (2006). Windows Mobile Security Software Fails The Test. Airscanner Corporation.

[2] Gupta, Gaurav (2005). Relative Locative system for a GSM Environment. Beedance Technologies.

[3] MediaWiki (2006). Mobile Computing. December 16th, 2006. <http://en.wikipedia.org/wiki/Mobile_computing > Tanggal Akses: 30 Desember 2006

[4] Satyanarayanan, M. (1996). Fundamental Challenges in Mobile Computing. School of Computer Science: Carnegie Mellon University.

[5] MediaWiki (2005). Smartphone. October 5th, 2005. <http://en.wikipedia.org/wiki/Smartphone > Tanggal Akses: 24 November 2005

[6] Finan, Terence (2002). Developing Applications For Windows Mobile-Based Smartphone. Pocket PC Technical Articles Juli 2002. Microsoft Corporation.

[7] Willassen, Svein Y. (2003). Forensics and the GSM mobile telephone system. International Journal of Digital Evidence Spring 2003 Volume 2 Issue 1.

[8] Wicaksono, Narenda (2006). Fungsionalitas AUREN dalam Proses Investigasi Pelacakan Pocket PC Phone dengan Menggunakan Perangkat Hukum di Indonesia. Institut Teknologi Bandung.

[9] Casey, Eoghan (2000). Digital Evidence and Computer Crime, First Edition., London: Academic Press.

[10] Dedo, Douglas (2004). Windows Mobile-Based Devices and Security: Protecting Sensitive Business Information. Windows Mobile White Paper. April 2004. Microsoft Corporation.

[11] Dellinger, Chris (2003). Design Robust Application that Take Advantage of Windows CE-powered Smartphone Devices. MSDN Magazine 2003. Microsoft Corporation.

[12] Intel Corporation. (2003). Intel Mobile Application Architecture Guide.

[13] Internet Standard Algorithm RFC 1321 <http://tools.ietf.org/html/rfc1321> Tanggal Akses: 20 September 2006.