

Tugas Akhir Mata Kuliah Security

**Aspek Security pada Penerapan
m-Commerce di Indonesia**

Nama : INDRA PURNAMA
NIM : 23203035

**Magister Teknik Teknologi Informasi
Departemen Teknik Elektro
Institut Teknologi Bandung
2005**

Daftar Isi

Abstrak	2
I. Overview m-Commerce	2
II. Sistem m-Commerce	3
III. Security	7
3.1 Security pada level jaringan	8
3.2 Security pada level transport	9
3.3 Security pada level Service	10
IV. Ancaman Security pada m-Commerce	10
4.1 Ancaman pada Level Service	11
4.2 Ancaman pada Level Jaringan GSM	12
V. Kesimpulan	14

Aspek Security pada Penerapan m-Commerce di Indonesia

Abstrak

Penetrasi penggunaan telepon seluler saat ini sangat tinggi, serta masih memiliki tingkat pertumbuhan yang tinggi pula. Tercatat saat ini terdapat 1 Miliar pengguna di seluruh dunia, dan 28 Juta pengguna di Indonesia. Fakta tersebut menjadikan telepon seluler sebagai smartcard reader dengan penetrasi terbesar di dunia. Sehingga merupakan langkah yang tepat apabila selanjutnya banyak entitas bisnis dan finansial yang kemudian mencoba untuk memberdayakan telepon seluler sebagai media transaksi yang baru. Namun demikian, diantara kelebihan yang dimilikinya, juga terdapat beberapa kelemahan dari jaringan seluler. Kelemahan tersebut terutama pada aspek security, dimana jaringan seluler pada awalnya hanya didesain untuk komunikasi, bukan transaksi, sehingga security pada jaringan seluler saat ini kebanyakan hanya efektif untuk mengamankan data komunikasi voice dan data, bukan untuk mengamankan transaksi.

I. Overview m-Commerce

m-Commerce merupakan proses transaksi yang dilakukan dengan menggunakan perangkat *mobile*. M-Commerce merupakan subset dari e-Commerce, yang didefinisikan sebagai proses transaksi yang dilakukan secara elektronik, baik melalui internet, smart card maupun perangkat mobile melalui jaringan seluler.

Pada umumnya, perangkat *end user* yang digunakan pada proses m-Commerce adalah sebagai berikut:

- Handphone
- Smart Phone
- PDA
- Laptop
- Earpiece (Personal Area Network)

Setiap perangkat memiliki karakteristik yang berbeda-beda sehingga dapat mempengaruhi tingkat penggunaannya, dan juga aplikasi / sistem m-commerce yang dapat digunakan. Karakteristik dari perangkat yang sangat mempengaruhi sistem m-commerce antara lain:

- Ukuran dan warna dari display
- Input device, seperti mouse dan keyboard / keypad
- Memory dan CPU
- Koneksi Jaringan dan Bandwidth
- Operating Sistem
- Smart Card reader

m-Commerce lahir setelah e-commerce yang pada umumnya dilakukan melalui media internet. Kelahiran m-Commerce tersebut terutama dipicu oleh tingginya tingkat penetrasi handphone di seluruh dunia. Dibandingkan sistem e-commerce lainnya, kelebihan m-Commerce adalah sebagai berikut:

- Ubiquity: pengguna dapat mengakses dari mana saja dan kapan saja.
- Security: pada umumnya handset dilengkapi dengan smart card reader dan smart card-nya itu sendiri. Sehingga dapat digunakan sebagai secret authentication key.
- Localization: memungkinkan diterapkannya location based services.
- Convenience: ukuran dan berat dari handset membuat pengguna nyaman dalam bertransaksi.
- Personalization: handphone merupakan perangkat yang bersifat personal, sehingga memungkinkan untuk menawarkan layanan / produk yang bersifat personal.

Namun demikian, diantara beberapa kelebihan seperti yang telah disebutkan di atas, m-Commerce juga memiliki beberapa kekurangan:

- Keterbatasan perangkat.
- Tingkat keberagaman perangkat, jaringan dan operating sistem yang sangat tinggi, membutuhkan standardisasi platform antar vendor. Antara lain telah diatasi oleh J2ME.
- Tingginya tingkat kehilangan / pencurian handphone.
- Bertambahnya tingkat kerawanan terhadap security ketika data ditransfer melalui air interface.

II. Sistem m-Commerce

Terdapat sejumlah besar payment sistem untuk e-commerce dan m-commerce. Beragamnya sistem tersebut disebabkan oleh faktor-faktor sebagai berikut:

1. Waktu Pembayaran.

Perbedaan yang terletak pada waktu pembayaran yang dilakukan oleh pengguna relatif terhadap waktu transaksi, yaitu apakah dilakukan pada saat transaksi, sebelum transaksi dilakukan atau setelah transaksi dilakukan.

2. Jumlah Pembayaran

Pada dasarnya dapat dibagi menjadi dua, yaitu transaksi dengan jumlah pembayaran besar, dan kecil. Terdapat perbedaan yang signifikan antara transaksi besar dan kecil. Pada transaksi dengan nilai yang besar, perlu dilakukan autentikasi melalui institusi finansial yang terpercaya. Sedangkan untuk transaksi kecil, autentikasi cukup hanya dilakukan pada level jaringan operator, antara lain melalui SIM Card.

3. Isu Anonim

Anonim berarti identitas pengguna / pelanggan tidak dapat diketahui oleh merchant. Terdapat sistem yang sepenuhnya anonim, anonim parsial atau bahkan tidak anonim. Masing-masing sifat tersebut dibutuhkan untuk transaksi yang berbeda-beda.

4. Validasi yang dilakukan secara online atau offline

Selain keempat isu utama tersebut, beragamnya sistem e-commerce dan m-commerce juga dipengaruhi oleh isu lainnya:

1. Biaya instalasi yang timbul di sisi customer dan merchant.
2. Performansi (respon time).
3. Biaya per transaksi.
4. Terjaminnya ACID (Atomicity, Consistency, Isolation, Durability).
5. Sistem yang berjalan di tingkat nasional atau internasional

Pada transaksi m-Commerce, tahap-tahap transaksi pada dasarnya adalah mirip dengan yang terjadi pada transaksi konvensional. Hanya saja pada kasus *remote payment*, pengiriman detail informasi transaksi dilakukan melalui jaringan seluler. Sehingga keamanan jaringan seluler juga menjadi perhatian khusus. Selain itu, proses pengiriman informasi transaksi juga melibatkan protocol browser, yang berupa WAP (Wireless Application Protocol), atau protocol sistem *messaging* seperti SMS (Short Message Service) dan USSD (Unstructured Supplementary Service Data). Keamanan dari setiap service tersebut juga harus diperhatikan untuk dapat mendukung sistem m-

commerce yang aman. Selain transaksi yang bersifat remote, m-Commerce juga dapat dilakukan untuk transaksi lokal, yang pada umumnya menggunakan koneksi Bluetooth, infrared atau RFID.

Secara umum, tahapan proses pada m-commerce dapat dibedakan menjadi 4 tahap sebagai berikut:

1. Set-up dan Konfigurasi

Proses ini termasuk instalasi aplikasi khusus pada handset yang akan digunakan pada m-commerce. Selain itu, untuk beberapa sistem m-commerce proses ini juga melibatkan proses pembelian atau penambahan nilai uang pada aplikasi tersebut.

2. Inisiasi Pembayaran

Pada tahap ini informasi pembayaran dikirimkan melalui jaringan seluler atau protokol wireless lainnya kepada merchant.

3. Authentikasi

Tahap ini merupakan tahap yang paling penting pada transaksi. Pada tahap ini diperiksa apakah pengguna memang berhak melakukan transaksi, serta memenuhi persyaratan finansial tertentu. Pada sebagian sistem pembayaran, proses ini melibatkan autentikasi berdasarkan SIM Card.

4. Penyelesaian Pembayaran

Proses ini dilakukan ketika pengguna telah berhasil di-authentikasi, demikian juga transaksi itu sendiri telah berhasil di-authentikasi. Analoginya pada proses transaksi konvensional adalah dengan dicetaknya bukti pembayaran.

Sistem pembayaran yang banyak digunakan pada e-commerce saat ini pada umumnya tidak dapat diterapkan pada m-commerce. Beberapa sistem yang dapat digunakan untuk m-commerce antara lain adalah:

1. Software electronic coin

Nilai uang disimpan dalam bentuk software di handset pengguna, sehingga pengguna memiliki control sepenuhnya terhadap penggunaan nilai uang tersebut. Electronic coin direpresentasikan dalam bentuk informasi nilai uang itu sendiri, serial number, tanggal kadaluarsa, dan signature dari institusi yang mengeluarkannya. Karena dalam bentuk software, sistem ini sangat mudah untuk diduplikat, dan proteksinya adalah dengan penggunaan serial number

yang benar-benar unik. Ketika akan melakukan transaksi, pengguna mentransfer coin kepada merchant, yang kemudian oleh merchant tersebut akan di-forward kepada Bank yang mengeluarkan coin tersebut untuk menghindari duplikasi dari penggunaan coin tersebut. Apabila ternyata memang nilai uang tersebut valid, maka nilai uang tersebut selanjutnya dipindahkan dari pengguna kepada merchant. Terdapat permasalahan dalam hal pembangkitan dan penyimpanan nilai uang, yang disebabkan oleh keterbatasan handset. Sehingga pada umumnya electronic coin dibangkitkan di perangkat lain, setelah itu baru disimpan di handset.

Kelebihan dari sistem ini adalah pengguna dapat sepenuhnya anonymous.

2. Hardware electronic coin

Pada sistem ini nilai uang disimpan pada suatu smart card yang tersimpan di dalam handset. Representasi nilai uang pada smart card tersebut sangat beragam, namun pada umumnya adalah berupa counter. Ketika akan melakukan transaksi, smart card pengguna dan smart card merchant saling melakukan proses autentikasi kepada pihak lainnya, kemudian akan terbangun suatu channel transaksi yang aman di antara kedua smart card tersebut. Selanjutnya nilai uang akan ditransfer dari pengguna kepada merchant. Kelebihan lain dari sistem ini adalah bahwa sistem ini dapat digunakan untuk transaksi yang sifatnya offline, yaitu pada POS (Point of Sales).

3. Background account.

Pada sistem ini, nilai uang disimpan pada pihak ketiga yang dapat dipercaya, baik itu berupa account kartu kredit, account bank atau account pada operator seluler. Pada suatu transaksi, dimana pengguna / pembeli menerima receipt, maka selanjutnya pengguna akan mengirimkan suatu pesan autentikasi dan otorisasi kepada merchant, untuk selanjutnya merchant melakukan otorisasi kepada institusi yang mengelola account tersebut. Selanjutnya masing-masing account pengguna dan merchant akan disesuaikan nilainya sesuai dari nilai transaksi. Terdapat beberapa sistem background account, yang memiliki fitur yang berbeda-beda sesuai kebutuhannya. Perbedaan tersebut antara lain adalah format pengiriman message dari pengguna, apakah plain text atau ter-enkripsi.

III. Security

Pihak-pihak yang terkait dalam transaksi mobile payment adalah pengguna (pembeli), operator jaringan, institusi financial dan merchant (penyedia produk / jasa yang akan dibeli pengguna). Seluruh pihak tersebut memiliki kebutuhan akan jaminan security sebagai berikut:

- Pengguna, menuntut dijaminnya security pada account-nya, dan juga privacy, sehingga pihak lainnya sedapat mungkin tidak mengetahui identitas pribadi pengguna.
- Operator jaringan seluler, merupakan fasilitator dari m-commerce, memiliki perhatian khusus dalam menyampaikan informasi transaksi secara aman melalui jaringannya.
- Institusi financial, memiliki perhatian khusus pada integritas dari sistem pembayaran, sehingga dapat mengurangi resiko terjadinya *fraud* atau *bad-debt*.
- Merchant, menuntut agar proses pembayaran menjadi mudah disisi pengguna, sehingga akan membangkitkan transaksi. Selain itu merchant juga menuntut agar pembayaran dari institusi financial dapat berlangsung dengan sempurna.

Security memegang peranan penting dalam m-commerce. Karena hanya dengan jaminan security m-commerce dapat dijamin *cost effective* sehingga layak untuk diselenggarakan. Elemen-elemen security yang perlu diperhatikan dalam m-commerce adalah sebagai berikut:

- *Authentikasi*, yang memungkinkan pihak fasilitator pembayaran (antara lain institusi keuangan) untuk memastikan bahwa pihak yang menggunakan sitem pembayaran adalah pihak yang berhak.
- *Confidentiality*, yang memastikan bahwa pihak lain yang tidak berhak tidak dapat mengakses data pembayaran.
- *Data Integrity*, yang memastikan bahwa data pembayaran tidak berubah setelah pengguna menyetujui seluruh detail transaksi.
- *Non-repudiation*, yang mengikat seluruh pihak yang terlibat sehingga tidak dapat menyangkal seluruh proses yang telah dilakukannya.

Transaksi m-commerce pada umumnya berlangsung melalui media transport yang disediakan oleh jaringan seluler. Sehingga perlu diperhatikan juga keamanan dari jaringan yang digunakan. Selain jaringan operator, perlu diperhatikan juga keamanan

dari handset dan aplikasi m-commerce yang digunakan. Namun demikian, terdapat beberapa keterbatasan yang diakibatkan oleh:

- Koneksi yang bersifat dinamik, melalui beberapa jaringan akses yang terkadang tidak aman atau tidak dapat dipercaya.
- Keterbatasan yang ditimbulkan oleh protokol komunikasi, antara lain bandwidth dan latency.
- Keterbatasan perangkat, antara lain daya dan kinerjanya.
- Belum matangnya teknologi *client*.

3.1 Security pada level jaringan

Security dari Teknologi Jaringan Mobile

- GSM
Merupakan sistem dengan pengguna terbanyak saat ini. Pada awalnya hanya mendukung koneksi circuit data 9,6 Kbps. Layanan saat ini SMS, WAP, GPRS, High speed CSD. Security pada GSM menggunakan IMSI (kode internasional pelanggan) dan Ki (kunci yang digunakan untuk autentikasi) yang disimpan di SIM Card. Encripsi air interface menggunakan symmetric key yang diturunkan dari Ki. Kelemahan utama dari GSM adalah bahwa jaringan inter operator tidak terenkripsi. Kelemahan lainnya adalah autentikasi hanya dilakukan satu arah, yaitu dari sisi jaringan kepada perangkat *end-user*, sehingga dimungkinkan terjadinya penyadapan oleh perangkat yang 'menyamar' sebagai BTS dari sisi perangkat *end-user*.
- UMTS
Pada jaringan UMTS telah dilakukan perbaikan terhadap aspek security dibandingkan yang dimiliki oleh jaringan GSM. Perbaikan tersebut mencakup proses autentikasi dan enkripsi data pelanggan. Proses autentikasi yang semula dilakukan secara satu arah, pada jaringan UMTS dilakukan secara mutual, yaitu dari network kepada handset dan dari handset kepada network. Sedangkan dari sisi pengamanan pesan atau percakapan yang dikirimkan oleh pengguna, proses enkripsi selalu dilakukan secara *end-to-end*, kecuali jika baik handset dan network sepakat untuk berkomunikasi tanpa enkripsi. *Integrity protection* digunakan untuk menjaga signaling message. UMTS menggunakan *algoritma chipper* yang baru dan *encryption keys* yang lebih panjang.

- Wireless LAN

Secara default tidak menerapkan security pada air interfacenya. Kemudian IEEE menerapkan WEP (Wired Equivalent Privacy), yang memberikan:

1. Autentikasi kepada Access Point.
2. Integrity dan Confidentiality dari MAC Frame.

- Blue tooth

Ad hoc piconet, pada personal *environment*, sangat potensial untuk m-Commerce. Pada link layer sekuriti dilakukan dengan *challenge-response* protocol untuk autentikasi dan *stream chipper algorithm* untuk user dan signaling data. Jika perangkat-perangkatnya tidak saling menukarkan key, maka yang ditukarkan adalah PIN yang harus sama, dapat dengan cara input manual pada handset maupun dengan cara mengimportnya dari aplikasi yang sama.

3.2 Security pada level transport

Kebanyakan transaksi berlangsung dengan tidak hanya melibatkan jaringan akses saja, tapi juga sering melibatkan jaringan yang dikelola oleh pihak ketiga. Sehingga diperlukan juga jaminan keamanan yang bersifat end-to-end.

SSL/TLS

Merupakan salah satu protocol yang paling banyak digunakan di internet saat ini. Salah satu penerapannya adalah HTTPS. SUN telah berhasil mengembangkan versi client side dari SSL untuk device dengan keterbatasan processing dan memory, dinamakan kilobytes SSL (KSSL). Walaupun tidak mendukung client side authentication, dan hanya mendukung beberapa chipper yang umum digunakan, namun kelebihan SSL adalah dapat dijalankan di atas platform J2ME, dengan hanya menghabiskan sedikit memory.

WTLS

WAP forum telah menstandarkan protocol security pada layer transport yang disebut WTLS, dan mengimplimentasikannya pada WAP 1. WTLS memfasilitasi sekuriti antara perangkat mobile dengan WAP Gateway, yang selanjutnya melakukan konversi kepada SSL / TLS. Sehingga memang belum memfasilitasi security yang sifatnya end-to-end, dan WAP gateway harus dapat dipercaya. Namun demikian, saat ini WAP forum telah mengusulkan suatu stack protocol WAP 2, yang identik dengan TCP/IP untuk media

wireless. Sehingga dengan demikian security yang sifatnya end-to-end dapat diselenggarakan.

3.3 Security pada level Service

SMS

Merupakan service yang paling banyak digunakan untuk transaksi saat ini, walaupun hanya dapat memfasilitasi maksimal 160 karakter. Pengirim dan penerima SMS diidentifikasi dengan menggunakan IMSI, sehingga keamanan layanan ini termasuk tinggi, karena didukung oleh keamanan GSM itu sendiri (keamanan SIM Card). Sehingga SMS dapat digunakan sebagai autentikasi, setidaknya pada jaringan GSM itu sendiri. Selanjutnya pesan SMS dikirimkan melalui *signaling plane* GSM, dimana tidak tersedia security yang sifatnya end-to-end, sehingga memang seluruh pihak yang terlibat pada m-Commerce harus percaya sepenuhnya kepada operator GSM.

SIM Tool Kit

Memungkinkan operator atau provider lain untuk membuat suatu aplikasi khusus yang tertanam di SIM Card. Aplikasi tersebut bertugas untuk mengirimkan, menerima, serta mengartikan sebuah SMS atau USSD. STK memungkinkan aplikasi pengirim (yaitu aplikasi yang terdapat pada SIM Card) untuk mengirimkan pesan yang sudah terproteksi kepada aplikasi penerima (yaitu pada server payment operator). Mekanisme security yang mungkin untuk diterapkan adalah:

1. Autentikasi
2. Integritas Informasi Transaksi
3. Integritas urutan transaksi dan deteksi pengulangan transaksi
4. Bukti Penerimaan dan eksekusi transaksi
5. Kerahasiaan Informasi

IV. Ancaman Security pada m-Commerce

Saat ini di Indonesia telah terdapat beberapa sistem m-Commerce. Aplikasi m-Commerce tersebut antara lain diterapkan pada layanan perbankan untuk membangun sistem mobile banking, serta layanan value added service yang dijalankan operator seluler. Layanan mobile banking pada umumnya melayani transfer antar rekening, pembayaran tagihan, serta pengaksesan informasi umum. Sedangkan value added service dari operator seluler pada umumnya adalah pembayaran tarif premium oleh

pelanggan yang digunakan untuk membeli informasi, barang atau jasa yang nilai nominal uangnya relative kecil.

4.1 Ancaman pada Level Service dan Aplikasi

Kebanyakan dari sistem m-Commerce tersebut pada umumnya berjalan di atas service SMS dan SIM Tool Kit. Sebagaimana telah dijelaskan di atas, service SMS keamanan aksesnya telah dijamin oleh jaringan GSM, melalui mekanisme IMSI. Namun demikian, dikarenakan di sisi merchant atau operator identitas yang digunakan untuk autentikasi hanya MSISDN (nomor handphone) pengirim SMS dan PIN yang disertakan pada isi pesan SMS, maka m-Commerce yang berbasis SMS menjadi tidak aman lagi. Hal tersebut disebabkan karena saat ini operator seluler di Indonesia seluruhnya telah melakukan interkoneksi dengan operator seluler di luar negeri. Sebagian dari operator seluler di luar negeri tersebut pada umumnya bekerjasama dengan pihak ketiga untuk memberikan layanan SMS Bulk dengan sender ID yang dapat diubah, baik dalam bentuk angka maupun alphanumeric. Hal tersebut berarti, pengguna dapat 'memalsukan' nomor handphone. Sehingga dengan demikian, satu-satunya pengamanan yang dapat diandalkan adalah PIN pengguna yang disertakan pada isi pesan SMS. Analoginya pada sistem kartu kredit atau kartu debit adalah hilangnya kartu tersebut, sehingga berpindah tangan ke pihak lainnya. Orang lain tersebut selanjutnya dapat menyalahgunakan kartu kredit atau debit dengan hanya menerka nomor PIN-nya. Layanan SMS Bulk dengan sender ID yang dapat diubah tersebut dapat diakses oleh pengguna di Indonesia hanya dengan mengakses website dari provider tersebut.

Namun demikian, ancaman ini hanya terjadi pada sistem m-Commerce yang berbasis Long Number, yaitu nomor handphone biasa (+628XXXXXXXXX). Sedangkan untuk sistem yang berbasis Short Number, yaitu nomor virtual 4 digit, ancaman ini tidak berlaku. Hal tersebut dikarenakan Short Number bersifat *local significant*, yang berarti nomor tersebut hanya bersifat unik pada jaringan operator yang sama, sehingga hanya dapat diakses oleh pengguna dari jaringan seluler yang sama. Sedangkan Long Number bersifat *global significant*, yang berarti nomor tersebut bersifat unik di seluruh dunia, sehingga dapat diakses oleh pengguna dari jaringan seluler manapun.

Kelemahan lain dari SMS *Plain Text* adalah bahwa pada jaringan operator seluler, pesan yang kita kirimkan dapat terbaca oleh operator, karena pada jaringan seluler proses encrispsi hanya dilakukan pada jaringan akses, yaitu dari BTS kepada handset. Sedangkan pada *core network* dan *microwave link* tidak dilakukan encrispsi. Hal tersebut berarti informasi penting yang digunakan untuk bertransaksi menjadi hilang sifat

kerahasiaannya. Sebagai solusi untuk menutupi kelemahan hingga saat ini hanya diatasi dengan jaminan keamanan dari operator seluler. Sehingga pada akhirnya pihak merchant dan pengguna memang harus mempercayakannya kepada operator.

Kelemahan tersebut tidak terjadi pada aplikasi yang berbasis SIM Tool Kit atau J2ME (Java 2 Micro Edition). Penyebab utamanya adalah karena pada aplikasi SIM Tool Kit dan J2ME kita dapat menambahkan faktor security tambahan, misalnya dengan cara melakukan enkripsi terhadap pesan yang akan dikirimkan melalui *bearer* SMS. Selain itu, format informasinya pun tidak bersifat transparan kepada pengguna, sehingga pengguna tidak dapat memanipulasi dengan cara mengirimkan SMS dari media lain (seperti yang dapat dilakukan pada sistem yang berbasis SMS *Plain Text*).

Pada implementasinya, aplikasi atau service di tingkat *user interface* ini akan digunakan untuk mengirimkan data transaksi, misalnya pada sistem banking atau *electronic coin*. Sehingga dibandingkan format plain SMS, pemanfaatan aplikasi SIM Tool Kit atau aplikasi J2ME adalah lebih baik, karena memungkinkan sistem pengiriman data transaksi tersebut untuk diintegrasikan dengan sistem payment yang digunakan, yang selanjutnya akan meningkatkan tingkat keamanan sistem payment tersebut.

4.2 Ancaman pada Level Jaringan GSM

GSM menjamin autentikasi dari pengguna kepada jaringan, yang berarti hanya pengguna yang memang terdaftar yang dapat mengakses jaringan GSM. Proses tersebut dilakukan melalui proses *challenge & response*, untuk menguji IMSI (nomor pelanggan internasional) dan Ki (kunci enkripsi) yang keduanya tersimpan pada SIM Card. Proses autentikasi tersebut hanya dilakukan satu arah, yaitu dari sisi jaringan kepada perangkat *end-user*. Sedangkan proses sebaliknya, yaitu autentikasi jaringan oleh pengguna tidak difasilitasi oleh GSM. Artinya terdapat kemungkinan ketidakamanan yang ditimbulkan akibat adanya unauthorized-BTS. Unauthorized-BTS adalah suatu perangkat yang 'menyamar' dengan bertindak seolah-olah sebagai BTS terhadap perangkat *end-user*, dan bertindak seolah-olah sebagai perangkat *end-user* terhadap BTS sesungguhnya. Kehadiran unauthorized-BTS ini bersifat membahayakan, karena selain dapat menyadap data pembicaraan juga dapat membangkitkan transaksi-transaksi palsu.

Kelemahan ini telah diatasi pada sistem 3G UMTS, dimana proses autentikasi dilakukan secara dua arah, yaitu dari perangkat *end-user* kepada jaringan, dan dari jaringan kepada perangkat *end-user*.

Kelemahan lain dari jaringan GSM adalah belum tersedianya security yang *end-to-end*. Sebagaimana telah disinggung sebelumnya bahwa enkripsi untuk layanan dasar GSM (yaitu SMS, voice dan WAP) hanya dilakukan pada hop terakhir jaringan GSM saja, yaitu pada jaringan akses. Sedangkan pada segmen jaringan lainnya tidak dilakukan pengamanan data. Kelemahan ini telah diatasi pada sistem 3G UMTS, dimana untuk layanan dasarnya telah dilengkapi dengan security *end-to-end*. Layanan dasar utama dari 3G UMTS adalah Mobile IP, sehingga pengamanannya dengan menggunakan IPSec.

V. Kesimpulan

Layanan dasar dari jaringan GSM / GPRS yang saat ini dioperasikan di Indonesia tidak cukup aman untuk digunakan sebagai media transaksi. Sehingga untuk memberikan layanan m-Commerce yang aman perlu melibatkan layanan tambahan yang dapat didukung oleh GSM / GPRS, seperti aplikasi SIM Tool Kit atau aplikasi J2ME over SMS / GPRS. Dengan demikian, akan terdapat mekanisme security tambahan yang sifatnya *end-to-end*. Security tambahan tersebut merupakan tanggung jawab dari aplikasi, dan bersifat transparan kepada jaringan GSM / GPRS. Aplikasi SIM Tool Kit dan J2ME juga memungkinkan untuk diterapkannya sistem pembayaran yang beragam, misalnya electronic coin, dengan tingkat keamanan yang baik.

Referensi

1. Schwiderci-Groche & Heiko Knospe; Secure m-Commerce; Information Security Group.
2. NetSec; Mobile Computing Security Threat; October 2004.
3. Nokia; Managing Security on Mobile Phone; April 2003.
4. Mobile Payment Forum; Enabling Secure, Interoperable and User Friendly Mobile Payment; December 2002.
5. Lucent Technologies; Deliver Secure Mobile Service; May 2002.
6. Trusted Computing Group; Security in Mobile Phones; 2004.
7. Ram Gopal Lakshmi Narayanan; Security in Mobile Internet; International Conference on Communication and Broadband Networking; 2004.