Daftar Isi

Strategi untuk Peningkatan *Security* Menghadapi Budaya Transaksi *Wireless* di Masyarakat

Benny Benyamin Nasution[1]
Politeknik Negeri, Kampus USU, Medan

ABSTRACT

Transactions utilising wireless technologies have been used and culturally accepted, but the awareness of security threats within those transactions seems to be inadequate. This paper specifically focuses on security strategies that should be used for increasing the security of transactions using wireless technologies. To achieve this objective, there needs to be a thorough analysis of security requirements and handlings. Due to some limitations existing in wireless networks, this paper presents how some security weaknesses can be resolved and improved on the application level. In order to present a satisfactory understanding overview of the implications of the security model, a serverless application (serverless network storage) is analyzed. It is proposed that an innovative model for security support for wireless networks, through which appropriate and sophisticated handlings can be achieved.

Key words: *data security, distributed system, network security, cellular phone network.*

Usaha untuk menangani transaksi *wireless* sudah dimulai. Dalam risetnya Khan and Spindler (Khan and Spindler, 2001) telah mendefinisikan beberapa jenis jaringan *wireless*. Contohnya, ada jaringan *wireless* yang terbentuk hanya melalui koneksi sederhana beberapa perangkat yang terhubung pada jaringan *wireless* dengan aplikasi tertentu. Dari hasil pengamatan diketahui bahwa kebutuhan akan jaringan *wireless* telah berkembang, dari hanya sekedar untuk bagi-bagi sumber daya, misalnya CPU atau *storage*, menjadi tujuan-tujuan bisnis. Selain daripada itu, aplikasi dan peralatan *wireless* diharapkan akan semakin fleksibel, menyebar, dan semakin kecil, baik pada penggunaan energi maupun sinyal. Akan tetapi, harapan seperti ini berpotensi melahirkan sejumlah risiko. Fleksibel dan menyebar telah diketahui akan memberikan kemungkinan lebih luas pada jaringan untuk mendapat ancaman (*threat*). Selain itu, penggunaan sumber daya yang kecil dapat memberikan peluang bahkan bagi suatu program kecil untuk memberikan serangan (*attack*). Begitu pula dengan kondisi sumber daya kecil ini memudahkan orang yang meskipun berpengetahuan dasar di bidang komputer dapat menghasilkan aplikasi yang dapat menghasilkan masalah-masalah. Oleh karena itu, suatu peningkatan konsep *security* khususnya untuk jaringan *wireless* sudah harus terus dikembangkan.

Security merupakan permasalahan yang sudah dijabarkan lengkap dalam dokumen RFC2828 (Shirey, 2000) dan X.800 (ITU-T Study Group VII, 1991). Dalam dua dokumen ini dijabarkan bahwa ada enam *security properties* yang harus dipenuhi saat mengelola *security*, yaitu: *availability*, *confidentiality*, *integrity*, *authentication*, *authorisation*, dan *non-repudiation*. Dari enam *properties* tersebut, tiga *properties* pertama berkaitan dengan data/informasi, sementara tiga *properties* lain berkaitan dengan pengguna data/informasi.

Availability berarti bahwa data/informasi harus dijaga/dijamin tersedia setiap saat diperlukan. *Confidentiality* maksudnya adalah isi dari data/informasi harus dijaga/dijamin agar hanya dapat diketahui oleh yang berhak saja. Integrity berkaitan dengan hal bahwa data/informasi dijaga/dijamin akan tetap sama dengan data/informasi tersebut pada saat dihasilkan. Selanjutnya *authentication* berarti pengguna data/informasi dijaga/dijamin benar pengguna semestinya. *Authorization* maksudnya bahwa pengguna data/informasi dijaga/dijamin memiliki hak pengelolaan data/informasi sesuai dengan seharusnya. Terakhir *non-repudiation* berarti bahwa penghasil data/informasi dijaga/dijamin tidak dapat mengingkari telah menghasilkan data/informasi tersebut.

Meskipun memiliki tujuan yang sama, para peneliti di bidang *security* memiliki pendapat-pendapat yang

[1] Korespondensi: Benny Benyamin Nasution. Politeknik Negeri Medan, Jl. Almamater No. 1, Kampus USU, Medan 20155. E-mail: bnasution@yahoo.com.

bervariasi dalam hal implementasi dan aplikasi. Beberapa peneliti percaya bahwa setiap perangkat *wireless* dapat menangani *security* (King, 2002). Oleh karena aplikasi perangkat *wireless* biasanya menggunakan jaringan Internet (TCP/IP), maka ketergantungan terhadap kualitas *security* jaringan Internet masih sangat tinggi (King, 2002; Wierzbicki et al., 2002). Selanjutnya, pada tingkatan tertentu masih diharapkan agar teknologi *wireless* yang lebih baru masih dapat berinteraksi dengan teknologi *wireless* yang lama. Sebagai konsekuensinya, teknologi *wireless* yang baru masih harus terus menggunakan mekanisme dan infrastruktur *security* yang lama (Kim et al., 2002; Wierzbicki et al., 2002). Sebelum masuk ke penanganan *security*, berikut ini akan dibahas terlebih dahulu jaringan *wireless*.

Jaringan Lapisan *Wireless*

Lapisan *wireless* menyediakan pelayanan-pelayanan (*services*) umum untuk aplikasi-aplikasi yang berada di lapisan/tingkatan atasnya. Lapisan ini umumnya terdiri dari modul-modul berikut ini: (1) *cluster* dan *identity management*; (2) *discovery*; (3) *communications*; (4) *security management*; dan (5) *routing*.

Cluster dan *Identity Management*

Perangkat-perangkat yang berkolaborasi membentuk jaringan *wireless* diatur kedalam *cluster-cluster* ukuran kecil. Kriteria dan algoritma yang digunakan untuk pembentukan dan pengaturan dijelaskan oleh Senaratna dan Khan (Senaratna & Khan, 2002). Modul ini menjalankan fungsi-fungsi yang terkait dengan: pembentukan *cluster*, pemilihan pimpinan *cluster*, fungsi-fungsi untuk memimpin *cluster*, dan penyimpanan data anggota *cluster*.

Aspek lain dari modul ini adalah menjalankan fungsi-fungsi manajemen identitas. Identitas dari tiap perangkat, sejauh ini sudah dilengkapi dengan kunci sandi (*key*) yang dihasilkan pada saat penginstalasian aplikasi. Biasanya kunci sandi yang digunakan adalah bilangan acak yang dikombinasikan dengan alamat perangkat tersebut di jaringan. Sebelum kunci sandi ini dilegitimasikan sebagai suatu bagian dari identitas yang valid (misalnya harus *unique*) bagi suatu perangkat, kunci sandi ini terlebih dahulu diperiksa melalui beberapa level proses pengujian. Saat suatu perangkat sudah dapat berinteraksi dalam kelompok (*cluster*), maka status validitas identitas dari perangkat ini perlahan-lahan akan meningkat. Semakin banyak perangkat lain terlibat dalam kelompok tersebut, semakin tinggi validitas identitas perangkat itu akan berubah. Hal ini berlaku demikian disebabkan pada banyak jaringan *wireless* tidak berisikan suatu pusat otoritas (misalnya *server*) yang akan mengatur dan mendistribusikan kunci sandi.

Discovery

Arsitektur *wireless* sebagian besar terdistribusi dan tidak memiliki perangkat pengelola yang tersentralisasi. Oleh karena itu, upaya untuk mengetahui perangkat-perangkat yang bergabung pada jaringan merupakan hal yang sangat penting. Secara alamiah ditinjau dari sisi kedinamisannya, perangkat yang bergabung pada jaringan *wireless* atau yang meninggalkan jaringan akan terus terjadi secara konstan. Modul *discovery* inilah yang bertugas mendeteksi dan mendata penambahan atau penghilangan perangkat pada jaringan. Beberapa solusi alternatif yang menggunakan teknik *discovery* seperti ini masih terus diteliti dan dikembangkan, misalnya yang menggunakan fasilitas *web services* (Nasution et al., 2003), atau memanfaatkan mekanisme pencarian pintar (*intelligent search mechanisms*). Modul *discovery* ini akan berinteraksi dengan *cluster database* untuk mendapatkan segala informasi tentang perangkat yang baru bergabung.

Communication

Modul ini mengatur interaksi dengan perangkat lain. Modul ini juga menyediakan beberapa mekanisme transportasi data sesuai dengan jenis interaksinya. Modul ini mengatur seluruh komunikasi untuk lapisan *wireless*. Selanjutnya, modul *commmunication* ini menyediakan satu *interface* bagi setiap aplikasi yang ada di atas lapisan ini. Oleh karena itu, meskipun tidak bersifat mutlak aplikasi-aplikasi tadi dapat menggunakan *interface* ini untuk keperluan komunikasinya. Modul *communication* ini juga menyediakan cara yang aman untuk transmisi data melalui penggabungannya dengan modul *security management*.

Security Management

Pada modul ini tersedia infrastruktur keamanan yang sesuai dengan lapisan jaringan *wireless*. Fungsi-fungsi utama dari modul ini dapat dikategorikan seperti berikut ini: (1) *key management*; (2) *encryption/decryption;* (3*) trust management*; dan (4) *integrity checker*. Begitupun perlu ditekankan bahwa seluruh keperluan keamanan

dari suatu aplikasi tidak dilayani melalui modul ini. Misalnya, keamanan penyimpanan bagi aplikasi yang berbasiskan penyimpanan tidak sepenuhnya dapat dilayani pada lapisan jaringan ini.

Key Management

Fungsi dasar dari *key management* adalah untuk mengatur pasangan kunci-kunci sandi perangkat yang akan digunakan pada modul *identity* management dan fungsi-fungsi keamanan lainnya. Fungsi-fungsi manajemen lainnya termasuk tanggal akhir masa berlaku suatu kunci sandi, menghasilkan kunci sandi baru, lalu sirkulasi dari kunci sandi. Sebagai tambahan, perangkat akan memperoleh setiap kunci sandi dari setiap perangkat lain yang berada dalam jaringan yang sama.

Encryption/Decryption

Modul menyediakan fungsi-fungsi enkripsi dan dekripsi yang diperlukan untuk mengamankan komunikasi. Fungsi-fungsi ini berkolaborasi dengan modul komunikasi. Kunci sandi diakses pada *key repository*. Segala informasi yang harus disandikan saat transmisi menggunakan fasilitas di modul ini. Oleh karena lapisan *wireless* dapat mendukung aplikasi-aplikasi yang berbeda, modul ini menyediakan beberapa skema enkripsi dan dekripsi termasuk *system* penanganan kunci sandinya. Berkaitan dengan enkripsi adalah *digital signature*. Segala informasi yang memerlukan *authentication* dapat di-*signed* secara digital oleh pembuat/pemilik data/informasi.

Trust Management

Kepercayaan (*trust*) adalah suatu kebutuhan penting dari sistem pengamanan. Menyediakan level *trust* yang sesuai dalam arsitektur jaringan *wireless* adalah suatu hal yang cukup menantang. Modul *trust management* bertugas menjaga level *trust* untuk perangkat-perangkat lain. Hal ini meniru prosedur yang digunakan manusia dalam menjabarkan *trust*.

Ada beberapa level dalam *trust* (Ye et al., 2001). Saat modul menemukan perangkat yang baru bergabung, modul akan mencari informasi tentang perangkat baru ini dari perangkat-perangkat yang sudah dipercaya sebelumnya. Pada awalnya, suatu perangkat yang baru bergabung akan diberikan level *trust* paling rendah, namun secara perlahan-lahan nilai itu dapat bertambah naik. Hal ini mencerminkan perambatan *trust*. Mekanisme seperti ini masih memiliki kelemahan, namun pengalaman ratusan tahun manusia menyatakan bahwa proses pembangunan *trust* dalam kelompok-kelompok masyarakat berfungsi dalam level yang dapat diterima.

Integrity Checker

Integrity checker dapat digunakan aplikasi untuk manajemen *integrity*. Suatu mekanisme *checksum* seperti MD5 dapat dimanfaatkan untuk tujuan ini. Fitur ini dapat digunakan untuk aplikasi-aplikasi yang dapat menjaga integritas data pada file yang disimpan dalam disk yang terdistribusi. Misalnya saat suatu aplikasi akan melakukan penyimpanan file pada lokasi jauh, modul dapat membuat *checksum* untuk file tersebut melalui mekanisme algoritma *one-way hash*. Selain daripada itu, *checksum* ini dapat di-*signed* secara digital menggunakan fasilitas yang tersedia pada modul *security*. Perangkat lain yang akan menggunakan file ini dapat memeriksa kesesuaian *checksum* untuk mengetahui kondisi integritasnya.

Routing Module

Modul *routing* berperan untuk perawatan dan penyebaran informasi *routing* melalui jaringan *wireless* menggunakan beberapa mekanisme *routing*. Data yang diperoleh menggunakan jaringan *ad-hoc* (Royer & Toh, 1999) termasuk juga algoritma-algoritma *dynamic routing* masih terus diteliti untuk menentukan kesesuaian dengan mekanisme *routing* pada *wireless cluster inter-communication*.

Kebutuhan *Security* untuk Jaringan *Wireless*

Banyak peneliti telah menyelidiki permasalahan *security* pada jaringan-jaringan *wireless* (King, 2002, Wierzbicki et al., 2002; Scott & Sharp, 2002; Yeager & Williams, 2002; Kim et al., 2002). Meskipun lapisan jaringan *wireless* yang dibahas di atas sudah menyediakan beberapa pelayanan untuk *security*, kekhawatiran mendasar adalah bahwa masih sulit sekali menjaga *security* pada lingkungan yang dinamis dan tidak terjamin seperti pada kebanyakan jaringan *wireless*.

Sebagai tambahan, kekhawatiran tersebut akan membesar apabila data penting dan sensitif sudah mulai dimasukkan dalam transaksi. Satu penyebab yang pasti dari kesulitan ini adalah sifat anonim

(*anonymous*) dari setiap perangkat (Cornelli et al., 2002). Kondisi seperti ini selanjutnya akan memberikan potensi pada keadaan yang rentan (Wierzbicki et al., 2002; Parameswaran et al., 2001, King, 2002; Kim et al., 2002). Bersumber dari kekhawatiran tadi, kebutuhan-kebutuhan untuk *security* telah dikelompokkan dalam dua bagian: (a) umum (untuk *wireless*); dan (b) spesial (untuk aplikasinya).

Kebutuhan *security* umum (untuk *wireless*): (1) saat berinteraksi dengan jaringan *wireless*, yang mana tanpa satupun perangkat bertindak sebagai pusat otoritas untuk memproteksi data, sangat perlu dipatuhi setiap perangkat agar memastikan tidak akan menghasilkan atau mentransfer sesuatu yang berpotensi membahayakan; (2) tidak ada satu perangkat pun yang melakukan pemalsuan identitas seolah-olah perangkat lain. Meskipun alamat IP bukan satu-satunya faktor penting dalam melakukan *authentication* suatu perangkat (Scott & Sharp, 2002), fakta menunjukkan bahwa alamat IP yang dimanipulasi dapat menimbulkan masalah dan dapat mengakibatkan kesemrawutan dalam trafik transaksi data. Oleh karena itu, pengujian *authentication* untuk alamat IP sangat diperlukan; (3) meskipun perangkat dapat meninggalkan dan bergabung dengan jaringan *wireless* sebebasnya, keberadaan jaringan wireless harus terus dijaga. Pada saat hanya ada satu perangkat yang masih tinggal dalam jaringan, maka perangkat tersebut harus diupayakan agar terus berada dalam jaringan; (4) setiap perangkat dan datanya hanya dapat dimonitor oleh perangkat lain yang sudah memilki otoritas. Sementara itu, perangkat lain tidak boleh memiliki hak sedikitpun untuk melihat isi dari data komunikasi. Beberapa peneliti juga telah merekomendasikan bahwa tiap dua perangkat yang berkomunikasi masing-masing harus memiliki mekanisme *security* untuk melindungi transaksinya (Kim et al., 2002, Parameswaran et al., 2001). Oleh karena itu, beberapa mekanisme security pada level aplikasi diperlukan; dan (5) mekanisme tambahan untuk menjaga rekaman reputasi atau kejadian-kejadian yang telah dialami oleh suatu perangkat, misalnya dengan menggunakan aplikasi *mobile agent*, merupakan hal yang penting (Cornelli et al., 2002). Jika kebutuhan ini dapat dicapai, maka jaringan *wireless* yang bersangkutan dapat mendukung satu dari enam *security properties*, yaitu *non-repudiation*.

Walaupun segala kebutuhan di atas umumnya mengatur seluruh enam komponen dasar *security* (*availability*, *confidentiality*, *integrity*, *authentication*, *authorisation*, dan *non-repudiation*), kelemahan, kerentanan, dan ancaman akan meningkat secara aktif pada saat aplikasi-aplikasi jaringan *wireless* ini mengakomodasikan transaksi yang penting dan sensitif. Berikut ini adalah poin-poin utama dari kebutuhan di atas: (1) berkaitan dengan kedinamisannya. Oleh karena perangkat dapat bergabung dan keluar jaringan dengan bebas, sangat sulit untu melakukan pengawasan terhadap aktivitasnya atau untuk mendeteksi kegiatan yang berbahaya (*malicious*). Pengguna yang berbahaya (*malicious* user) dapat memilih waktu kerja yang tepat untuk menjalankan aksinya (Parameswaran et al., 2001) sehingga akan sulit terpantau. Oleh karena itu tidak dijamin bahwa aplikasi akan berada di jaringan terus-menerus. *Authentiacation* dan *availability* adalah dua aspek utama *security* yang akan terganggu dari kondisi ini; (2) pengguna-pengguna yang belum berpengalaman dalam permasalahan *security* terlihat mudah sekali menjadi target suatu penyerangan (*attacks*) pada saat melakukan transaksi yang penting dan sensitif. Perangkat yang berbahaya dapat dengan mudah mengelabui perangkat yang belum berpengalaman tanpa mampu untuk dideteksi. Dalam kasus ini, komponen *confidentiality*, *authentication*, dan *authorisation* tidak lagi terpenuhi. Situasi seperti ini adalah suatu paradox, sebab pada satu sisi diharapkan agar status anonim pada setiap perangkat sangat diharapkan pada jaringan *wireless*. Pada sisi lain, perangkat pengendali juga diperlukan untuk memenuhi syarat elemen *security* yang disebut di atas. Sebagai tambahan lagi, jelas terlihat bahwa berat untuk mewujudkan dukungan pada elemen *security non-repudiation* jika setiap perangkat tetap *anonym*; dan (3) kelemahan *security* pada jaringan *wireless* berikutnya adalah tidak terbatasnya jumlah perangkat yang dapat bergabung pada suatu jaringan *wireless*. Pada beberapa aplikasi seperti musik, film, dan file *sharing*, semakin banyak perangkat yang bergabung pada jaringan akan semakin menguntungkan bagi seluruh perangkat. Akan tetapi, oleh karena keterbatasan jaringan secara fisik, trafik yang melebihi kemampuan jaringan dalam menerima koneksi, permintaan, dan data, dapat menyebabkan kemacetan (King, 2002). Hal ini akhirnya dapat menimbulkan kondisi *denial of service* yang berarti aspek *security availability* dan mungkin juga *integrity* tidak lagi terjamin. Dalam kondisi seperti ini *quality of service* (QoS) tidak lagi dapat divalidasikan.

Kebutuhan *security* khusus (untuk aplikasi): (1) untuk menjaga informasi tentang sumber data, dan untuk melindungi *non-repudiation*, hanya pemilik dan pembuat data yang dapat memvalidasi *authentication* dan *integrity* data; (2) oleh karena data

merupakan entitas yang terpenting dalam aplikasi penyimpan data (SNS), hanya pemilik data yang dapat melakukan modifikasi terhadap data; (3) seperti pada *system file* yang lain dalam sistem kerjasama sumber daya, hanya pemilik data yang dapat menganugerahkan hak penggunaan data tersebut kepada perangkat lain; (4) meskipun kemampuan untuk mengetahui penyebab dari kesalahan modifikasi penting untuk dimiliki, tetap saja merupakan hal yang penting untuk menyembunyikan lokasi fisik atau replika data, bahkan dari pemiliknya sendiri. Mekanisme seperti ini akan mencegah pengguna yang berbahaya, sebagai pemilik data, untuk menseleksi tujuan dari serangan yang akan dilakukan; (5) untuk menjaga pemerataan distribusi dan untuk menghindari terjadinya kelebihan beban sehingga dapat menggangu *integrity* dan *availabitliy* (King, 2002; Parameswaran et al., 2001), pada aplikasi penyimpanan terdistribusi (SNS) besar kapasitas maksimum yang dapat digunakan oleh suatu perangkat harus lebih kecil dari besar kapasitas maksimum yang dapat disediakan perangkat itu; dan (6) ada aplikasi penyimpanan terdistribusi, jika suatu perangkat kehilangan kapasitas penyimpanan lokalnya, maka harus ada suatu mekanisme untuk menjaga replikanya, namun tidak harus kekal.

Seperti yang sudah disinggung di atas, satu dari aplikasi yang memanfaatkan jaringan *wireless* adalah *serverless network storage* (SNS). Pada aplikasi SNS, setiap perangkat yang bergabung akan mendapatkan kapasitas media penyimpanan yang tersebar pada perangkat-perangkat lain yang membagi (*sharing*) kapasitas media penyimpanan lokal mereka masing-masing. Meskipun ada perangkat yang tidak menyediakan kapasitas lokalnya sama sekali, aplikasi SNS tetap membolehkan perangkat ini untuk bergabung dalam aplikasi. Kondisi ini tentu dapat dimanfaatkan oleh pengguna yang berbahaya untuk membebani seluruh kapasitas penyimpanan yang ada sehingga akan menimbulkan kondisi *denial of service*. Ini berarti telah mengganggu aspek *security availability*. Selanjutnya, merupakan hal yang sulit untuk mengukur dan mengendalikan beban trafik termasuk beban penyimpanan (King, 2002; Parameswaran et al., 2001), bahkan meskipun ada satu perangkat bertindak sebagai koordinator. Alasan utamanya adalah bahwa koordinator juga merupakan perangkat dalam jaringan yang suatu saat juga akan keluar dan masuk jaringan secara dinamis. Akibatnya, koordinator yang baru tidak akan mampu mewarisi/mengambil alih pengetahuan yang dimiliki oleh koordinator sebelumnya.

Permasalahan penting *security* lainnya pada SNS adalah data itu sendiri. Oleh karena replika data disimpan dan didistribusikan pada banyak media penyimpanan perangkat lain, koordinator dan pemilik data akan mengalami kesulitan dalam melindungi replika agar tidak mengalami penyerangan (*attack*) berpotensi dari pemilik media penyimpanan. Alasan yang memungkinkan hal ini dapat terjadi bukan karena pemilik media penyimpanan tertarik hanya untuk melakukan tindakan berbahaya (*malicious act*), namun ada kemungkinan pemilik media penyimpanan tersebut tidak rela media penyimpanannya digunakan oleh perangkat lain tanpa batas waktu yang pasti.

Di samping alat-alat bantu yang umum untuk *security*, seperti kriptografi, *public key infrastructure* (PKI), *secure socket layer*/*transport layer security* (SSL/TLS), dapat digunakan pada aplikasi SNS, ada beberapa tambahan perhatian yang diperlukan juga untuk dipertimbangkan saat mengimplementasikan SNS, yaitu: (1) bagi suatu perangkat, untuk dapat mengurangi sejumlah risiko tersebut di atas yang kemungkinan besar dapat dialami, perangkat itu perlu mengambil manfaat melalui adanya peningkatan saling percaya (*mutual trust*) satu sama lain dengan perangkat-perangkat lain (Kim et al., 2002; Parameswaran et al., 2001); (2) oleh karena setiap perangkat harus menjaga keamanannya sendiri seperti melalui suatu mekanisme *security* pada level aplikasi, perangkat juga harus membentuk kerja sama dengan perangkat-perangkat lain, misalnya menjalankan group *authentication*; (3) setiap perangkat sebaiknya menjaga keadilan untuk rasio pelayanan yang digunakan dibandingkan dengan pelayanan yang disediakan (Parameswaran et al., 2001), dan tidak berlebihan, agar *availability* dapat terjamin; dan (4) beberapa level mekanisme proteksi *security* yang berbeda diperlukan, sebab ada beberapa level kepentingan data yang berbeda tersimpan.

Solusi *Security* Model untuk Aplikasi SNS pada Jaringan *Wireless*

Pada bagian ini akan dibahas tentang bagaimana mengatur *security*, khususnya untuk aplikasi SNS, jika diimplementasikan dalam jaringan *wireless*. Berkaitan dengan pembahasan sebelumnya di atas, dapat dinyatakan bahwa *security* pada aplikasi SNS dapat diatur apabila kriteria berikut ini terpenuhi: (1) SNS tersedia dan dapat diakses oleh siapapun melalui internet; (2) SNS tidak memiliki satupun

otoritas sentral, misalnya *server*; (3) keberadaan dan kontribusi suatu perangkat dalam aplikasi SNS secara logis tersembunyi atau tidak pasti; dan (4) SNS dapat digunakan untuk menyimpan data pribadi, atau mendistribusikan *software* sensitif.

Sebelum menangani beberapa permasalahan utama, penting untuk mempertimbangkan asumsi berikut ini yang berkaitan dengan aktivitas SNS di jaringan *wireless*. Asumsi pertama adalah bahwa suatu perangkat tiap saat dapat *login* ke aplikasi SNS hanya satu kali. Jika koneksi lain dari perangkat yang sama memaksa untuk *login* secara konkuren, perangkat yang bertindak sebagai koordinator memiliki kewajiban untuk memutuskan koneksi sebelumnya. Asumsi berikutnya adalah, sebelum melakukan suatu transaksi suatu perangkat harus mengupayakan atau menggunakan proteksi *security* tambahan pada data. Kondisi ini akan melindungi data dari gangguan perangkat lain. Asumsi terakhir adalah, setiap perangkat harus teregistrasi pada *cluster* lokal sebelum diizinkan menggunakan media penyimpanan. Kondisi ini akan memungkinkan adanya *monitoring* perangkat-perangkat dalam *cluster* lokal.

Bagian di bawah ini akan membahas permasalahan *security* jaringan yang berkaitan dengan aplikasi SNS. Pada pembahasan akan dielaborasi juga kemungkinan-kemungkinan solusinya, seperti perangkat terpercaya, pengurangan risiko (kerentanan dan ancaman), dan data terpercaya.

Security Jaringan

Tersebar di mana-mana (*ubiquity*) merupakan sumber ke-rentan-an yang umumnya dirasakan oleh pemakai bersumber dari Internet. Penyerangan (*attack*) dapat dibangkitkan dari mana saja (Kim et al., 2002, Parameswaran et al., 2001), dan pelakunya dapat mengubah posisi kerja secara terus-menerus sehingga lokasi pasti keberadaannya sulit untuk diidentifikasi. Oleh karena koordinator dari SNS memerlukan selang waktu tertentu untuk sinkronisasi pembuatan replika, pemilik data tidak akan memiliki kesempatan untuk memverifikasi dan melindungi *integrity* dari replika yang dibuat. Satu bagian dari replika dapat ditukar saat proses sinkronisasi dalam selang waktu beberapa detik tanpa dapat terdeteksi. Selain daripada itu, setiap perangkat memiliki kesempatan untuk menggali data illegal melalui mode pemakai pasif. Ini berarti bahwa suatu perangkat dapat meregistrasi media penyimpanan lokalnya hanya untuk menggali data dari perangkat lain.

Satu dari masalah utama dalam menangani *security* jaringan dalam SNS adalah terkait pada ketiadaan otoritas sentral. Artinya, setiap perangkat harus melindungi dirinya sendiri dari serangan berbahaya. Oleh karena itu penting bagi perangkat-perangkat di suatu *cluster* untuk membentuk komunitas perangkat terpercaya (*trusted community*) (Kim et al., 2002; Parameswaran et al., 2001). Komunitas seperti ini dapat dibentuk secara independen dari aplikasi SNS. Beberapa dari pelayanan dapat juga diatur pada lapisan *wireless*. Koordinator dari SNS kemudian dapat mendistribusikan replika dari data anggota komunitas hanya ke anggota komunitas terpercaya lain. Akhirnya, proses registrasi yang sebelumnya diuraikan di atas dapat digunakan untuk membantu seluruh anggota komunitas mengatur proses *authentication* dan *authorisation* secara efisien.

Akan tetapi, membangun kepercayaan melalui pembentukan komunitas belum dapat memenuhi keseluruhan kelengkapan *security* (*security properties*), sebab pemilik media penyimpanan yang berbahaya atau kerusakan *hardware* dapat merusak data. *Availability* dapat juga menjadi permasalahan disebabkan koordinator SNS tidak mampu melakukan monitoring secara terus-menerus (Parameswaran et al., 2001; Cornelli et al., 2002). Untuk mengatasi permasalahan ini, perangkat memerlukan aplikasi tambahan yang sering disebut *mobile agent* untuk mengawasi *integrity*. Mobile agents ini dapat dijalankan dan dihentikan secara sporadis oleh perangkat dan melaporkan hasil temuannya kepada pemilik data untuk tindakan berikutnya. Apabila tingkat sensitivitas data menjadi kritis, maka *mobile agents* harus dijalankan lebih sering. Hanya *mobile agents* yang dibangkitkan oleh perangkat terpercaya yang dapat mengunjungi suatu perangkat, dan perangkat yang dikunjungi harus menjaga agar *mobile agent* tersebut tetap aktif.

Dalam suatu jaringan *wireless*, setiap perangkat memiliki hak yang lebih kurang sama. Perangkat-perangkat dalam suatu *cluster* harus menentukan siapa yang akan menjadi koordinator. (Senaratna & Khan, 2002). Proses yang sama dapat digunakan untuk menghukum perangkat yang berbahaya. Bentuk hukuman yang memungkinkan dapat berupa pemutusan hubungan atau penolakan dari seluruh *cluster*. Mekanisme yang sama juga dapat diterapkan untuk perangkat yang menggunakan SNS secara berlebihan. Pada kasus ini, hukuman bukan berupa pemutusan hubungan melainkan hanya pembatasan kapasitas media penyimpanan yang dapat digunakan. Begitupun, pada saat perangkat

ini sudah dapat meningkatkan kapasitas media penyimpanan lokalnya dan meregistrasikannya ke koordinator, maka perangkat ini akan terbebas dari hukumannya. Untuk mewujudkan hal ini diperlukan *database* tentang perangkat yang harus dijaga terus-menerus.

Simpulan

Di sini disimpulkan bahwa, melalui beberapa pengembangan pada teknologi jaringan *wireless* seperti menyebar di mana-mana, kesederhanaan, permasalahan *security* tidak hanya muncul pada jaringan namun juga pada aplikasi. Pada tulisan ini disampaikan hasil investigasi pada permasalahan *security* jaringan yang sejauh ini belum begitu banyak didiskusikan. Oleh karena itu, di sini dicoba dijustifikasi kondisi *security* jaringan *wireless* termasuk satu dari aplikasinya, yaitu SNS. Di sini juga diajukan beberapa solusi-solusi potensial yang dapat mengatasi permasalahan yang selama ini ada.

Oleh karena kebutuhan berbeda-beda antar satu aplikasi dengan aplikasi lain, model yang ditawarkan di atas belum dapat mewakili rancangan detil untuk mengamankan jaringan *wireless*. Lebih sesuai bahwa model *security* di atas menyediakan batasan kerja dalam menghadapi kebutuhan *security* khususnya dalam jaringan *wireless* dan aplikasinya. Tulisan ini juga merekomendasikan penggunaan mobile agent dalam jaringan *wireless* sebagai suatu entitas yang dapat menyediakan fitur-fitur manajemen *security*.

Daftar Pustaka

Cornelli, F., Damiani, E., Vimercati, S.D.C.D., Paraboschi, S. & Samarati, P. (2002) *Choosing reputable servents in a P2P network. the eleventh international conference on World Wide Web.* Honolulu, Hawaii, USA: ACM Press.

ITU-T Study Group VII (1991) *Security architecture for Open Systems Interconnection for CCITT applications (ITU-T Rec. X.800)*. International Telecommunication Union (ITU).

Khan, A.I. & Spindler, R. (2001) *A Blueprint for Building Serverless Applications on the Net*. Melbourne, Australia: School of Network Computing.

Kim, W., Graupner, S. & Sahai, A. (2002) A secure platform for peer-to-peer computing in the internet. In: *January 3–6 2001. HICSS. Proceedings of the 35th Annual Hawaii International Conference on System Sciences.*

King, M.M. (2002) Transforming the reliability, *security* and scalability of it communications through the pervasive deployment of serverless software infrastructure VO. In: 5–7 September *2002. (P2P 2002). Proceedings of the Second International Conference on Peer-to-Peer Computing.*

Nasution, B.B., Kendall, E.A., Khan, A.I. & Dospisil, J. (2003) Contributions of Web Services-Technology for Improving Resource Management of Real-Time Multimedia on the Internet. In: *The 14th Information Resources Management Association (IRMA) International Conference.* Philadelphia, Pennsylvania, USA: IRMA International. 440–443.

Parameswaran, M., Susarla, A. & Whinston, A.B. (2001) P2P networking: an information sharing alternative. *Computer* **(34):** 31–38.

Royer, E.M. & Toh, C.K. (1999) A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. *IEEE Personal Communications, April.*

Scott, D. & Sharp, R. (2002) Abstracting application-level web *security*. *The eleventh international conference on World Wide Web.* Honolulu, Hawaii, USA: ACM Press.

Senaratna, S.N. & Khan, A.I (2002) An autonomous *cluster*ing algorithm for Serverless Peer-to-Peer Systems. *Proceedings of the 6th International Conference on High Performance Computing in Asia Pacific Region.* Bangalore, India: Springer Verlag. 371–378.

Shirey, R. (2000) *Internet Security Glossary (RFC2828)*. [Accessed 23 July 2005*]* http://www.ietf.org/rfc/rfc2828.txt?number=2828.

Wierzbicki, A., Strzelecki, R., Swierczewski, D. & Znojek, M. (2002) Rhubarb: a tool for developing scalable and secure peer-to-peer applications. In: 5-7 September *2002. (P2P 2002). Proceedings. Second International Conference on Peer-to-Peer Computing.* Linköping, Sweden: IEEE. 144–151.

Ye, N., Emran, S.M., LI, X. & Chen, Q. (2001) Statistical process control for computer intrusion detection. *DARPA Information Survivability Conference & Exposition II, 12–14 June 2001. DISCEX '01. Proceedings.* Anaheim, California, USA: IEEE. 3-14.

Yeager, W. & Williams, J. (2002) Secure peer-to-peer networking: the JXTA example. *IT Professional,* (**4):** 53–57.