ANALISIS KEAMANAN PADA PROTOKOL *PAIRING* BLUETOOTH

Andrew Pratomo Budianto – NIM : 13505046

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : andrewpratomo@gmail.com

Abstrak

Kemajuan teknologi sedikit demi sedikit telah membawa manusia melewati era dimana kabel menjadi penghubung komunikasi antar perangkat keras. Salah satu teknologi yang berperan dalam hal ini adalah Bluetooth. Teknologi Bluetooth memberikan kelebihan – kelebihan mulai dari menggantikan kabel alat – alat elektronik di rumah sampai sistem jaringan sederhana. Teknologi Bluetooth memanfaatkan frekuensi radio ISM 2.4 GHz yang bebas lisensi. Oleh karena transmisi data berjalan di atas udara, maka terdapat ancaman terhadap data tersebut. Salah satunya, penggunaan layanan berbasis teknologi Bluetooth di area publik dalam menyediakan Bluetooth link untuk Bluetooth peers yang belum dikenal.

Terlepas dari banyaknya protokol pertukaran kunci berbasis kunci publik yang ada, pengamanan pada dua buah perangkat nirkabel umumnya menggunakan kunci simetri untuk alasan efisiensi. Konsekuensinya adalah penggunaan protokol yang dijumpai sehari – hari, seperti Bluetooth pairing menjadi kurang aman, kunci privat dapat dengan mudah didapat dari protokol komunikasi yang berlangsung.

***Kata kunci**: Bluetooth pairing, Bluetooth security,* Bluetooth, enkripsi, dekripsi, kriptografi kunci simetri.

1. Pendahuluan

Bluetooth merupakan sebuah teknologi komunikasi wireless yang memanfaatkan frekuensi radio ISM 2.4 GHz untuk menghubungkan perangkat genggam secara terpisah (handphone, PDA, computer, printer, dan lain-lain) dengan jangkauan yang relatif pendek. Perangkat-perangkat genggam yang terpisah tersebut dapat saling bertukar informasi atau data dengan menggunakan Bluetooth.

Teknologi Bluetooth diusulkan oleh Ericsson dan kemudian bersama-sama dengan IBM, Intel, Nokia, dan Toshiba membentuk Bluetooth Special interest Group (SIG) pada tahun 1998 yang kemudian diikuti oleh perusahaan besar seperti Microsoft, 3Com, Lucent, dan Motorola. Nama Bluetooth diambil dari nama raja Denmark, Harald Bluetooth. Tujuan dari perancangan Bluetooth adalah sebagai teknologi yang murah, handal, berdaya rendah, dan efisien.

2. Aplikasi layanan Bluetooth

Protokol bluetooth menggunakan sebuah kombinasi antara circuit switching dan packet switching. Bluetooth dapat mendukung sebuah kanal data asinkron, tiga kanal suara sinkron simultan atau sebuah kanal dimana secara bersamaan mendukung layanan data asinkron dan suara sinkron. Setiap kanal suara mendukung sebuah kanal suara sinkron 64 kb/s. Kanal asinkron dapat mendukung kecepatan maksimal 723,2 kb/s asimetris, dimana untuk arah sebaliknya dapat mendukung sampai dengan kecepatan 57,6 kb/s. Sedangkan untuk mode simetris dapat mendukung sampai dengan kecepatan 433,9 kb/s.

Sebuah perangkat yang memiliki teknologi wireless bluetooth akan mempunyai kemampuan untuk melakukan pertukaran informasi dengan jarak jangkauan sampai dengan 10 meter (~30 feet). Sistem bluetooth menyediakan layanan komunikasi point to point maupun komunikasi point to multipoint.

Produk bluetooth dapat berupa PC card atau USB adapter yang dimasukkan ke dalam perangkat. Perangkat-perangkat yang dapat diintegerasikan dengan teknologi bluetooth antara lain : mobile PC, mobile phone, PDA (Personal Digital Assistant), headset, kamera, printer, router dan sebagainya. Aplikasi-aplikasi

yang dapat disediakan oleh layanan bluetooth ini antara lain : PC to PC file transfer, PC to PC file synch (notebook to desktop), PC to mobile phone, PC to PDA, wireless headset, LAN connection via ethernet access point dan sebagainya.

3. Keamanan Bluetooth

Teknologi Bluetooth menggunakan mekanisme keamanan pada lapisan aplikasi dan lapisan saluran. Selain itu, penggunaan mekanisme seleksi hop sekitar 1.600 hop/detik menghindarkan interferensi dengan piconet atau perangkat ISM lain dan skema pengatur daya keluaran untuk mengatur konsumsi daya pada perangkat mobile sehingga mengurangi jangkauan penyebaran sinyal radio sesuai keperluan transmisi data.

Secara umum, terdapat tiga jenis metode keamanan yang ditetapkan oleh spesifikasi Bluetooth yaitu:

1. Authentication
   Suatu proses di dalam mengenali perangkat yang akan diajak berkomunikasi.
2. Confidentiality
   Suatu proses di dalam melindungi informasi yang bersifat sensitif/ pribadi.
3. Authorization
   Suatu proses di dalam mengatur akses ke sumber daya yang ada.

3.1 Mode Pengamanan Bluetooth

Berdasarkan prosedur keamanan yang digunakan Bluetooth dibagi ke dalam tiga mode keamanan sebagai berikut:

3.1.1 Security mode 1 (tanpa pengamanan)

Pada mode keamanan 1, suatu perangkat tidak akan melakukan prosedur keamanan. Fungsi-fungsi keamanan seperti authentication dan encryption tidak digunakan. Mode ini disebut juga “promiscuous mode” dimana sembarang perangkat Bluetooth dapat melakukan hubungan dengannya. Mode ini ditujukan untuk aplikasi yang tidak memerlukan pengamanan seperti pertukaran “business card”.

3.1.2 Security mode 2 (pengamanan pada tingkat layanan)

Pada mode ini prosedur pengaman dilakukan setelah pembentukan saluran di level logical link control dan adaptation protocol (L2CAP). L2CAP terletak di data link layer dan menyediakan layanan data bersifat connection-oriented dan connectionless ke layer di atasnya. Pada mode ini, security manager mengatur akses ke layanan dan perangkat. Security manager tersentralisasi mengatur kebijakan di dalam pengaturan akses dan hubungan dengan protokol dan perangkat lain. Berbagai kebijakan pengamanan dan level “trust” dalam pembatasan akses dapat diterapkan terhadap aplikasi dengan persyaratan kemananan yang berbeda-beda yang bekerja secara parallel. Pada mode ini, diterapkan pengamanan authorization dimana pengguna tertentu hanya dapat mengakses ke layanan tertentu saja.

3.1.3 Security mode 3 (pengamanan pada tingkat *link*)

Pada mode ini dilakukan prosedur pengaman di tingkat saluran sebelum pembentukan suatu saluran dan tidak berhubungan dengan prosedur keamanan di layer aplikasi. Fungsi-fungsi pengamanan authentication dan ebncryption diterapkan pada mode ini. Mode ini didasarkan pada penggunaan secret link key yang digunakan secara bersama-sama oleh sepasang perangkat Bluetooth yang saling berkomunikasi. Suatu pairing procedure digunakan untuk menghasilkan key ini ketika dua peragkat saling berkomunikasi untuk pertama kalinya.

3.2 Bluetooth Security Manager

Merupakan suatu komponen Bluetooth yang berfungsi untuk menentukan kebijakan dan fitur-fitur keamanan yang harus diterapkan ketika permintaan suatu hubungan dibuat. Security manager melakukan authentication, enkripsi, dan sebagainya berdasarkan layanan, jenis perangkat, dan tingkat trust perangkat.

Security manager memerlukan informasi berkaitan dengan perangkat dan layanan sebelum mengijinkan akses ke suatu layanan. Informasi tersebut tersimpan di dalam dua database yaitu device database dan service database. Device database menyimpan informasi yang berhubungan dengan jenis perangkat, level trust, panjang link key yang digunakan untuk enkripsi. Service database menyimpan informasi yang berhubungan dengan authentication, authorization, dan enkripsi suatu layanan. Selain itu juga menyimpan informasi ruting untuk layanan.

3.3 Bluetooth Link Key

Link key adalah suatu urutan angka acak sebesar 128 bit yang digunakan secara bersama-sama oleh dua atau lebih hubungan komunikasi .

Terdapat empat jenis link key yaitu:

1. Combination key KAB
   Dihasilkan dari unit A dan unit B yang digunakan untuk tingkat keamanan yang lebih.
2. Unit key KA
   Diperoleh dari instalasi perangkat Bluetooth unit A. Digunakan ketika perangkat ingin mengakses ke kelompok user yang besar.
3. Master key Kmaster
   Digunakan ketika parangkat master ingin melakukan tranmsisi ke beberapa perangkat sekaligus.
4. Initialization key KInit
   Digunakan padas saat proses inisialisasi. Berfungsi untuk melindungi paraleter inisialisasi ketika ditransmisikan.
5. Encryption key
   Encryption key mempunyai besar yang bervariasi antara 1 sampai 16 byte dan dinegosiasikan oleh kedua belah pihak yang saling berhubungan.

Encryption key dihasilkan dari link key. Ketika link manager mengaktifkan enkripsi, encryption key dihasilkan. Encryption key selalu berubah setiap kali perangkat Bluetooth masuk dalam mode enkripsi.

4. Bluetooth Pairing

Bluetooth pairing adalah proses yang terjadi ketika dua perangkat Bluetooth setuju untuk berkomunikasi satu sama lain dan mebentuk sebuah kanal komunikasi. Ketika dua perangkat Bluetooth ingin membentuk suatu hubungan komunikasi yang membutuhkan authentication, maka akan dilihat apakah terdapat link key diantaranya. Jika ada, maka akan langsung memproses authentication protocol. Sebaliknya, maka akan dibuat suatu initialization key yang akan digunakan bersama-sama berdasarkan PIN yang dimasukan pada kedua perangkat tersebut.

Untuk memulai proses pairing Bluetooth, sebuah kata kunci (*passkey*) harus dipertukarkan di antara dua perangkat yang bersangkutan. *Passkey* tersebut adalah kode yang sama dan dimiliki oleh kedua perangkat Bluetooth, sebagai bukti bahwa kedua pengguna setuju untuk melakukan *pairing* satu sama lain.

Proses yang terjadi kurang lebih dapat dijabarkan sebagai berikut:

1. Perangkat Bluetooth A mencari perangkat Bluetooth lain yang berada dalam jangkauan.
2. Perangkat Bluetooth A meminta perangkat Bluetooth B untuk memasukan kata kunci (*passkey*).
3. Perangkat Bluetooth A mengirim passkey pada perangkat Bluetooth B.
4. Perangkat Bluetooth B mengirim *passkey* kembali pada perangkat Bluetooth A.
5. Perangkat Bluetooth A dan B sudah terhubung dan dapat melakukan komunikasi data.

5. Keamanan dalam Bluetooth Pairing

Pengamanan komunikasi *digital* sering menggunakan enkripsi kunci simetri dan kode autentifikasi pesan. Hal ini memberikan kelebihan dari segi kecepatan dan keamanan. Namun, membentuk koneksi ideal seperti ini memerlukan persetujuan terhadap kunci privat. Persetujuan kunci privat dalam koneksi yang kurang aman merupakan tantangan yang cukup besar. Solusi awal yang kurang praktis dijabarkan pada tahun 1975 oleh Merkle. Pada tahun 1976, Diffie dan Hellman memberikan solusi baru yang bekerja dengan baik, bila dua pihak yang ingin membentuk koneksi dapat berkomunikasi melalui kanal yang terautentifikasi dengan baik yang menjamin integritas pesan.

Permasalahan yang terjadi adalah, untuk mengautentifikasi protokol Diffie-Hellman diperlukan komputasi yang tidak mudah. Karena protokol ini menghasilkan pesan yang cukup panjang, dan autentifikasi tersebut umumnya dilakukan secara manual oleh manusia. Salah satu solusi singkat adalah dengan memperkecil informasi ini, yang dengan kata lain membuat suatu algoritma *hash* dan hanya mengautentifikasi *digest* pada protokol transkrip. Jumlah data yang dikirim dengan cara ini dapat dikurangi dari ribuan bit menjadi 160 bit saja. Namun, *collision resistant hash-function* cukup rentan belakangan ini karena algoritma MD5, RIPEMD, SHA, SHA-1, dll. Sudah tidak seaman seperti pada beberapa tahun yang lalu. Terlebih lagi, 160 bit masih merupakan jumlah yang besar untuk diautentifikasi oleh manusia. Solusi lain menggunakan pesan yang lebih singkat telah dikirim oleh Pasini dan Vaudenay, menggunakan

fungsi *hash* yang menghindari *second preimage attack* (seperti MD5). Solusi lain adalah protokol MANA, protokol ini dapat mengurangi jumlah informasi yang diautentifikasi berkurang menjadi 20 bit, namun protokol ini mengasumsikan hipotesis yang lebih kuat pada kanal terautentifikasi. Beberapa protokol berbasis Diffie-Hellman juga dipublikasikan tanpa analisis keamanan yang kuat.

Solusi yang cukup menjanjikan pada akhirnya dipublikasikan oleh Vaudenay. Protokol ini hanya membutuhkan 20 bit untuk diautentifikasi dan berbasis pada *commitment scheme*. Autentifikasi dengan cara ini cukup murah (tidak menggunakan kriptografi kunci publik) dan terbukti cukup aman. Oleh karena pertimbangan di atas, dapat dikatakan karena *key agreement* merupakan fondasi dari kriptografi kunci publik, maka membuat komunikasi yang aman dengan kanal terautentifikasi tidak dapat diselesaikan dengan komputasi yang lebih murah dari algoritma kunci publik secara umum.

Standar Bluetooth menggunakan asumsi yang sedikit berbeda. Asumsikan terdapat kanal pribadi antara dua perangkat yang melibatkan peran manusia. Tentunya kanal ini harus digunakan untuk pengiriman data dengan jumlah bit sesedikit mungkin. Hal ini, secara prinsip, memungkinkan penggunaan autentifikasi berbasis *key agreement*. Proposal yang pertama dipublikasi tanpa pembuktian keamanannya adalah milik Bellovin dan Merritt pada tahun 1992. SRP adalah protokol lain yang cukup terkenal dan dapat digunakan di atas RFC 2945, dipublikasikan pada tahun 1998 oleh Wu. Analisis keamanan dilakukan melalui penelitian yang panjang oleh Bellare dan Rogaway. Pada akhirnya, protokol lain dipublikasikan pada tahun 2001 oleh Katz, Ostrovsky, dan Yung. Tiap protokol tersebut sayangnya tidak lebih murah dibanding protokol Diffie-Hellman.

4. Solusi

Menurut Bluetooth Special Interest Group, 8-digit PIN diperlukan ketika akan melakukan pairing pada dua perangkat Bluetooth. Kurang dari itu maka proses pairing akan rentan terhadap ancaman *hacker*.

Karena perangkat Bluetooth hanya memiliki jangkauan yang pendek, dan proses pairing hanya dilakukan oleh dua buah perangkat lunak, kebanyakan pengguna menganggap proses ini cukup aman. Namun, belum lama ini ditemukan sebuah jenis serangan pada perangkat Bluetooth, yang memaksa dua buah perangkat menjadi *unpaired*. Ketika pengguna melakukan proses *pairing* kembali, *hacker* dapat menyadap proses tersebut sekaligus PIN yang dipertukarkan.

Salah satu solusi yang paling aman saat ini adalah melakukan proses *pairing* pada tempat yang jauh dari jangkauan publik, dan menggunakan PIN sepanjang 8-digit.

DAFTAR PUSTAKA

[1] Gunapi Halim, Chairisni Lubis, Prawito Prajitno. Simulasi Kunci Elektronik dengan Enkripsi melalui Bluetooth pada Ponsel.

[2] Hahnsang Kim, Walid Dabbous, Hossam Afifi. (2005). *A Bypassing Security Model for Anonymous Bluetooth Peers*.

[3] Judge, Peter. (2005). Bluetooth needs long PINS for security. http://news.zdnet.co.uk/security/0,1000000189,39205871,00.htm. Tanggal akses: 18 Mei 2009 pukul 20:00.

[4] Munir, Rinaldi. Diktat Kuliah IF5054 Kriptografi. Departemen Informatika ITB. 2005.

[5] Philipus, Bayu Murthi. Sistem Keamanan Bluetooth

[6] *Specification of the Bluetooth System*, version 1.2., 5 November 2003.

[7] Vaudenay, Serge. *Key Agreement based on Symmetric-Key Cryptography*.