JURNAL DASI ISSN: 1411-3201
Vol. 11 No. 1 Maret 2010

TEKNIK DOCUMENT OBJECT MODEL (DOM) UNTUK MANIPULASI DOKUMEN XML

Kusnawi
Dosen STMIK AMIKOM Yogyakarta

Abstraksi

Extensible Markup Language (XML) merupakan media yang sangat penting untuk representasi, pertukaran, dan pengaksesan data yang bersifat independen multi platform tanpa tergantung pada teknologi yang digunakan. DOM atau disebut sebagai Document Object Model adalah model yang digunakan untuk memanipulasi dokumen XML, yaitu sebuah platform dengan bahasa yang netral yang memungkinkan suatu program atau script secara dinamis mengakses dan memperbaharui suatu dokumen, struktur dan berbagai gaya dari sebuah dokumen.

Document type definition atau sering disebut DTD, memungkinkan format yang unik untuk setiap dokumen xml. DTD berfungsi untuk mendefinisikan tipe dokumen XML. Seperti halnya deklarasi variable, deklarasi fungsi dan deklarasi tipe data pada bahasa pemrograman atau scripting untuk memastikan bahwa data yang diterima aplikasi itu adalah data yang valid.

Untuk mendemontrasikan dengan menggunakan visual basic, bagaimana memanipulasi dengan DOM adalah memfaatkan fungsi DOMXML, parser XML yang membaca keseluruhan isi dari XML hingga end tag *ditemukan, kemudian diterjemahkan dan diolah datanya.*

Kata kunci : *XML, DTD, DOM, DOMXML*

Pendahuluan

Kemampuan memanipulasi data biasanya sangat tergantung dari tool atau sistem yang digunakan. DBMS adalah sistem pengelolaan suatu data yang tidak terlebas dari kelebihan dan kekurangan, tergantung dari vendor dan berbagi macam permasalahan dari mulai kecepatan, kapasitas penyimpanan dan bentuk struktur data serta arsitektur didalamnya.

XML menyediakan format untuk mendeskripsikan data terstruktur atau terurut. Fasilitas yang disediakan XML membuat isi (*content*) suatu data menjadi lebih mudah dipahami. Format data XML, dapat diolah dengan berbagai *tool* pengolah data yang berbeda-beda dan untuk tujuan yang berbeda-beda. Misal, suatu program yang satu digunakan untuk menampilkan data, sedang program yang lain untuk mengedit data.

Bentuk struktur XML yang terdiri dari elemen-elemen yang bebas di definisikan menjadikan kemudahan dalam melakukan manipulasi konten istilah lainnya disebut sebagai XML parser dari mulai membaca, membuat dan memanipulasi dokumen XML.

***Extensible Markup Language* (XML)**

XML, singkatan dari *Extensible Markup Language*, adalah bahasa *markup* yang dirancang untuk penyampaian informasi melalui *website* dan juga dapat digunakan untuk pertukaran informasi antar sistem *database*. Bahasa *markup* (*markup language*) merupakan bahasa pemrograman untuk menandai suatu data.

keuntungan menggunakan XML dapat menyederhanaan aplikasi, dimana *database* yang ditulis dalam XML dapat diakses di mana saja dan memudahkan aplikasi dalam mengolah data karena dapat menghemat memori. Kemampuan dalam mendefinisikan tag-tag di dalam dokumen XML dapat secara leluasa menerangkan isi data. Berbeda dengan HTML yang digunakan untuk menampilkan data, XML tidak didesain untuk menampilkan data, XML didesain untuk menyimpan dan pertukaran data antar format dari system yang tidak kompatibel. Konversi data ke XML dapat mereduksi kompleksitas dan membuat data dapat dibaca oleh aplikasi yang bebeda-beda.

XML dapat digunakan untuk menyimpan data dalam suatu *file* atau *database*. Aplikasi dapat dibuat untuk menyimpan dan memanggil informasi dari *file* penyimpan untuk menampilkan data tersebut. XML bersifat independen terhadap *hardware, software* dan aplikasi, menyebabkan aplikasi dapat mengakses *file* XML sebagai

sumber data, seperti mengakses *database*. Data dapat digunakan untuk hampir seluruh jenis mesin pembaca data.

Dokumen XML berupa *file plaintext* secara umum dibagi menjadi dua bagian yaitu prolog dan elemen dokumen. Prolog berisikan tentang pendekalarasian XML dan komentar. Elemen dokumen XML terdiri dari tag pembuka dan tag penutup yang memenuhi standar *well formed* diantaranya adalah :

1) Setiap *tag* pembuka harus ditutup dengan *tag* penutup
2) Tidak boleh ada elemen yang *overlapping*
3) Setidaknya ada satu elemen utama dan Penulisan atribut harus di antara tanda petik ganda (").

***Document Type Definition* (DTD)**

Dokumen XML harus memenuhi spesifikasi dalam *Document Type Definition* (DTD) untuk memastikan validitasnya. DTD adalah deklarasi tipe dokumen, berisi deklarasi yang mendefinisikan elemen, atribut dan fitur-fitur lain dokumen. DTD diletakkan dibagian *prolog* dokumen, dimulai dengan tulisan <!DOCTYPE Nama DTD>, dimana Nama menyatakan nama elemen dokumen. DTD berisi simbol [diikuti serangkaian deklarasi *markup*, diikuti dengan simbol].

Deklarasi *markup* menjelaskan struktur logika dokumen, yaitu mendefinisikan elemen, atribut dan fitur lain dokumen. DTD boleh tidak ditulis, namun menyebakan dokumen XML tersebut tidak dapat diperiksa validitasnya. Beberapa elemen-elemen penting dari DTD adalah:

DOCTYPE – root elemen DTD.

Deklarasi DOCTYPE menjelaskan tipe dokumen XML. Syntax: <!DOCTYPE NAME CONTENT>**.** NAME semestinya sama dengan nama root elemen di dokumen XML. content dapat dimasukkan dengan 2 cara: pertama secara inline (menguraikan secara langsung) atau melalui referensi luar. Referensi luar atau external reference dapat berupa file yang terpisah dan di refer melalui URL. Referensi ini memakai keywords SYSTEM dan PUBLIC.
Contohnya:
<!DOCTYPE FAMILY SYSTEM

http://www.amikomnet.com/dtd/file2.dtd>
<!DOCTYPE FAMILY PUBLIC "//amikomnet//DTD//EN"
http://www.amikomnet.com/dtd/file2.dtd>

ELEMENT

Tujuan dari keyword ini menentukan bila nama dari ELEMENT dapat dipakai di document type. Contoh syntax: <!ELEMENT NAME CONTENT> Istilah CONTENT meng-spesifikasikan apa yang dapat dimasukkan antara tag pembuka dan tag penutup. Tapi ini tidak termasuk attribut-attribut yang mungkin terpakai di elemen.

- EMPTY – isi yang kosong. Ini berarti diantara tag pembuka dan tag penutup tidak boleh mempunyai isi (termasuk spasi). Contoh: <!ELEMENT nama EMPTY>. Berarti nama tidak dapat mempunyai isi.
- ANY – jika suatu elemen dideclare sebagai ANY, berarti isi dari elemen ini adalah elemen lain.
  Contoh dari declaration ANY: <!ELEMENT nama ANY>.
  Berarti
  pemakaian di XML adalah:
  <nama><DECLARASI_ELEMEN_2 /></nama>
- #PCDATA – elemen hanya dapat memiliki karakter data yang di-parse. Karakter data dapat berupa teks apa saja asalkan tidak mempunyai child elements (bagian dari elemen).
  Contoh: <!ELEMENT nama (#PCDATA)>

ATTLIST

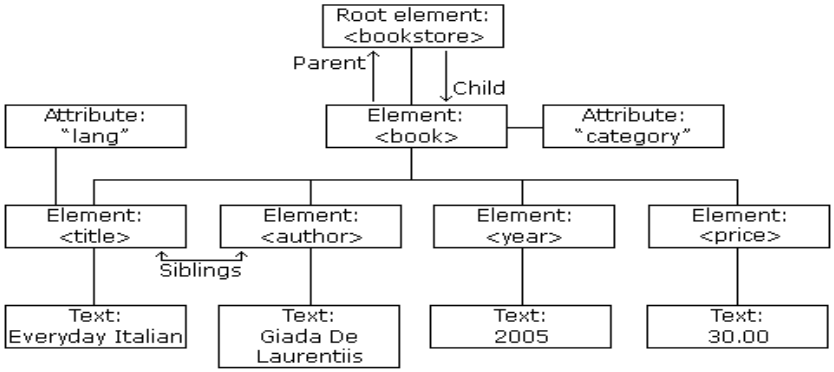
Syntax ATTLIST adalah untuk attribut yang dapat dipakai di dalam declared element. Syntax ini berupa seperti:
<!ATTLIST NAME
ATT_NAME TYPE DEFAULT
...>

XML DOM

Dokumen XML adalah dokumen terstruktur, untuk mengakses datanya, kita harus menggunakan pengurai (parser). Menguraikan dokumen XML dapat dilakukan melalui DOM (*Dokumen Object Model*) atau SAX (*Simple API XML*).

XML *Parser* sebagai pengurai XML berbentuk pustaka atau *software library* yang memberikan layanan-layanan bagi aplikasi yang akan membaca dan mengambil data di dalam dokumen XML. Pengurai XML ini menetapkan *Application Programming Interface* (API) tertentu untuk berinteraksi dengan program aplikasi yang menggunakannya dan mendefinisikan data model dari sebuah dokumen XML kepada aplikasi yang menggunakan pengurai tersebut.

DOM menggunakan struktur data yang disebut *DOM Document Tree*, suatu struktur pohon di memori yang serupa dengan dokumen XML yang sedang diurai. Terdapat satu *node* untuk setiap elemen XML dengan tipenya masing-masing. Dalam DOM, dokumen XML memiliki tipe *document*. Elemen-elemen di dalam dokumen tersebut umumnya bertipe *Element*. Berbagai atribut yang dimiliki oleh elemen diwakili oleh obyek-obyek bertipe *Attr*. Komentar dan elemen yang berisi teks diwakili oleh *CharacterData*



Gambar 1. XML DOM tree

Elemen terluar dari suatu dokumen, yang disebut *root node*, bukan merupakan bagian dari dokumen itu sendiri. Sebuah dokumen hanya memiliki satu *node* yang menjadi *root node*. Dokumen yang tidak mempunyai *root node* dikatakan sebagai dokumen kosong (*blank document*). DOM menggunakan *Interface Definition Language*(IDL) untuk mendefinisikan antarmuka berorientasi obyek (DSO) pada komponen-komponen perangkat lunak dan tidak bergantung pada suatu bahasa pemrograman tertentu, sehingga XML *Parser* dengan standar DOM dapat menggunakan berbagai bahasa pemrograman.

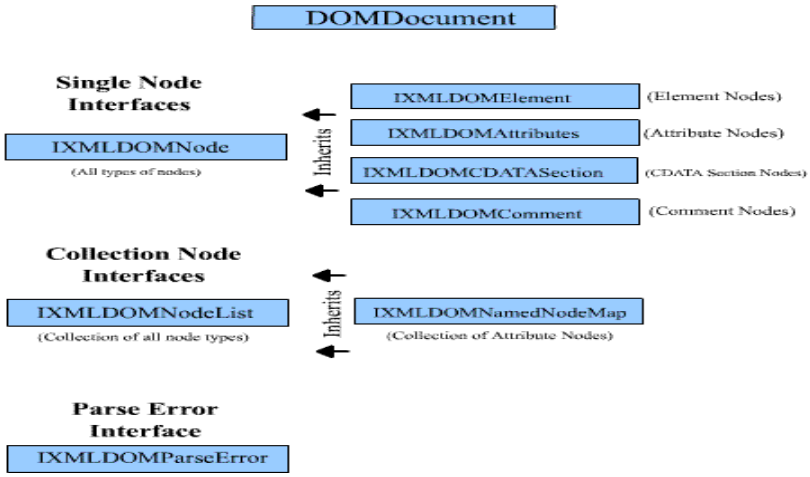
Pembahasan

Manipulasi Dokumen XML dengan DOM

Untuk memanipulasi struktur data pohon yang dihasilkan melalui *parser* diperlukan sebuah *interface* standar bagi pemrogram untuk menambah simpul, menghapus simpul, maupun mengubah isi sebuah simpul, aplikasi yang digunakan adalah dengan menggunakan Visual Basic.

Untuk mengakses data XML dengan Visual Basic, Microsoft menyediakan file MSXML.DLL. File MSXML.DLL menyediakan pustaka fungsi-fungsi yang berhubungan dengan Model Objek Dokumen XML. Melalui Model Objek ini Visual Basic dapat membaca data XML.

Diagram berikut ini adalah gambaran hirarki interface yang digunakan untuk memanipulasi XML :



Gambar 2. *MSXML DOMDocument Interfaces*

Rancangan Program

Sebelum membuat program, untuk melakukan manipulasi dengan DOM XML, diperlukan sumber data beruba dokumen XML dan DTD untuk menentukan validasi *well formed* pada dokumen XML. Berikut adalah contoh dokumen XML dan DTD yang digunakan.

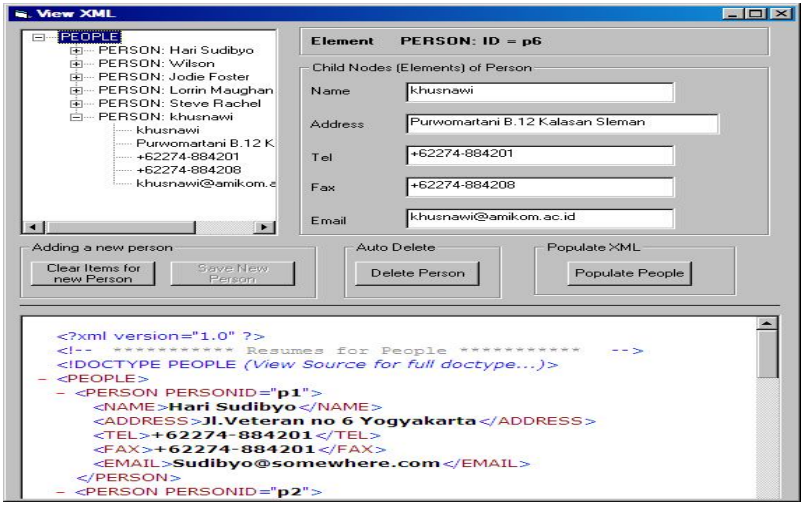
```
<?xml version="1.0"?>
<!-- ********** Resumes for People ********** -->
<!DOCTYPE PEOPLE SYSTEM "people.dtd">
<PEOPLE>
        <PERSON PERSONID="p1">
                <NAME>Hari Sudibyo</NAME>
                <ADDRESS>Jl.Veteran no 6 Yogyakarta</ADDRESS>
                <TEL>+62274-884201</TEL>
                <FAX>+62274-884201</FAX>
                <EMAIL>Sudibyo@somewhere.com</EMAIL>
        </PERSON>
                <PERSON PERSONID="p6">
                <NAME>khusnawi</NAME>
                <ADDRESS>Purwomartani Kalasan Sleman</ADDRESS>
                <TEL>+62274-884201</TEL>
                <FAX>+62274-884208</FAX>
                <EMAIL>khusnawi@amikom.ac.id</EMAIL>
        </PERSON>
</PEOPLE>
```

Gambar 3. Dokumen person.xml

```
<!ENTITY INA   "Indonesian">
<!ELEMENT PEOPLE ( PERSON+ ) >
<!ELEMENT PERSON ( NAME, ADDRESS, TEL, FAX, EMAIL ) >
<!ATTLIST PERSON PERSONID ID #REQUIRED>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT ADDRESS ( #PCDATA ) >
<!ELEMENT TEL ( #PCDATA ) >
<!ELEMENT FAX ( #PCDATA ) >
<!ELEMENT EMAIL ( #PCDATA ) >
```

Gambar 4. Format DTD untuk people.dtd

Tag XML Person PersonID menunjukan root elemen yang menunjukan identitas yang berbeda pada setiap elemen pada dokumen XML yang bersifat *autoincrement* pada fungsi DTD `<!ELEMENT PEOPLE ( PERSON+ ) >`.



Gambar 5. Contoh Hasil program

Kesimpulan

XML sebagai dokumen berbasis text dengan struktur yang menyerupai data struktur pohon diperlukan metode manipulasi untuk setiap node dari mulai *root element* sampai dengan *child element*. DOM XML sebagai parser XML dapat menguraikan dokumen XML dengan bahasa pemrograman atau script yang netral, dengan memperhatikan formed DTD untuk well formed setiap elemen XML. DOM menyediakan representasi dokumen secara terstruktur, dimungkinkan untuk merubah isi dan presentasi visual.

Daftar Pustaka

Kusnawi,Transformasi Dokumen XML untuk Proses Database dengan menggunakan Visual basic dan SQL Server. Skripsi tahun 2002

www.xml.com, di akses September 2009

http://www.w3schools.com/dom/default.asp , diakses september 2009

JURNAL DASI ISSN: 1411-3201
Vol. 11 No. 1 Maret 2010

WIRELESS SECURITY

M. Rudyanto Arief
STMIK AMIKOM Yogyakarta

Abstract

As the number of wireless networks increased, so too did the need for a wireless networking standard. 802.11 belongs to the Institute of Electrical and Electronics Engineers (IEEE) 802 family of standards for local and metropolitan area networks and wireless LANs

Keywords: *wireless LAN, wifi (wireless fidelity), access point, passive attack, active attack, tools, policies, MAC address, MAC filtering.*

Pendahuluan

Jaringan tanpa kabel (wireless LAN) saat ini semakin banyak digunakan oleh perusahaan dalam mendukung proses bisnis perusahaan tersebut. Meningkatnya jumlah penerapan teknologi jaringan wireless LAN tersebut tidak terlepas dari banyaknya keunggulan yang di tawarkan oleh teknologi ini. Kelebihannya diantaranya fleksibilitas yang ditawarkan, karena untuk menerapkan teknologi wireless LAN tidak terkendala masalah topologi/ kondisi tempat. Teknologi ini dapat diterapkan di mana saja dengan jangkauan sinyal yang cukup baik tergantung kualitas perangkat wireless LAN yang digunakan. Seiring dengan banyaknya pengguna dari teknologi jaringan berbasis tanpa kabel ini, maka semakin banyak pula pihak-pihak yang mencoba untuk melakukan "kejahatan" terhadap jaringan ini. Hal ini dapat dilihat dari banyaknya perangkat lunak/ tool yang diciptakan untuk melakukan serangan terhadap jaringan wireless baik itu jenis serangan aktif maupun jenis serangan pasif. perangkat lunak seperti ini biasanya di distribusikan melalui internet secara gratis dan ada juga beberapa yang berbayar. Sehingga diperlukan sebuah metode pengamanan yang tepat untuk mengatasi permasalahan keamanan untuk jaringan wirelessLAN.

Gambar 1. Arsitektur Jaringan Wireless

Jaringan wireless sangat rentan terhadap serangan, hal ini disebabkan karena jaringan dengan teknologi ini tidak dapat dibatasi oleh sebuah gedung seperti yang ada di jaringan berbasis kabel yang terlindungi oleh tembok didalam sebuah gedung dimana jaringan berbasis kabel tersebut terpasang. Sinyal frekuensi radio yang digunakan oleh jaringan wireless dalam melakukan proses transmisi data didalam jaringan tersebut dapat saja dengan mudah di terima/ di tangkap oleh pengguna komputer lain selain pengguna jaringan wireless tersebut hanya dengan menggunakan kartu jaringan wireless yang kompatibel/ cocok dengan jaringan wireless tersebut yang terpasang pada komputer pengguna komputer tersebut.

Celah keamanan pada jaringan wireless dapat dibagi kedalam 2 (dua) jenis serangan, yaitu: serangan pasif (passive attack) dan serangan aktif (active attack).

Pembahasan

Serangan Pasif (Passive Attack)

Serangan pasif adalah jenis serangan yang sesungguhnya tidak membahayakan terhadap sebuah sistem jaringan. Jenis serangan ini tidak menyebabkan hilangnya sumber daya dalam sebuah jaringan maupun menyebabkan kerusakan terhadap sebuah sistem jaringan yang di serang menggunakan jenis serangan ini. Sumber daya yang terdapat dalam sistem jaringan diantaranya berupa data, bandwidth

jaringan, printer, memori dalam sebuah komputer, unit pengolah (prosesor) dan masih banyak lagi. Intinya jenis serangan ini hanya melakukan pengamatan terhadap semua sumber daya yang terdapat dalam sebuah sistem jaringan komputer. seperti memantau lalu lintas jaringan sebuah sistem jaringan komputer. Informasi yang dihasilkan dari hasil pengamatan tersebut sangat bermanfaat bagi pihak yang tidak berhak untuk melakukan penyerangan selanjutnya terhadap sistem tersebut. sehingga jenis serangan ini sangat sulit untuk di deteksi oleh pengelola sebuah sistem jaringan komputer. Komunikasi jaringan tanpa kabel biasanya menggunakan frekuensi gelombang radio umum yang tidak terdaftar yang dapat di akses oleh siapapun dengan menggunakan kartu jaringan yang kompatibel. sehingga untuk jaringan jenis ini sangat mudah untuk di sadap dengan menggunakan teknik “sniffing” atau “wardriving”. Saat ini banyak “sniffer” menggunakan software seperti NetStumbler dengan kombinasi antena yang saling bekerja bersama dengan kartu jaringan tanpa kabel (wireless) untuk mendeteksi jaringan “access point” (AP) yang berada dalam jangkauan dan sinyalnya dapat diakses kartu jaringan tanpa kabel tersebut. Kemudian traffic data yang terjadi didalam jaringan wireless tersebut di tangkap oleh “sniffer” tersebut untuk kemudian di analisis dengan menggunakan tool seperti Microsoft Network Monitor untuk sistem operasi microsoft windows atau menggunakan Linux TCPDump untuk sistem operasi Linux.

Gambar 2. Jenis Serangan Pasif (Passive Attack)

Program seperti NetStumbler selain dapat digunakan untuk mendeteksi jaringan access point yang terdapat dalam jangkauannya juga dapat digunakan untuk menampilkan informasi yang terdapat pada Service Set Identifiers (SSID) dan informasi perusahaan pembuat access point tersebut. Sehingga jika Access Point tetap di konfigurasi masih menggunakan pengaturan SSID default yang disertakan oleh perusahaan pembuat ketika access point dibeli, maka jaringan wireless yang menggunakan perangkat access point tersebut sangat rentan terhadap masalah keamanan.

Jika SSID berisikan informasi mengenai organisasi yang menyediakan layanan jaringan wireless tersebut atau mungkin saja jaringan tersebut tidak menggunakan metode pengamanan dengan cara enkripsi seperti Wireless Equivalent Privacy (WEP) yang mampu melakukan enkripsi terhadap semua traffic data yang terjadi didalam jaringan wireless tersebut, jika hak tersebut terjadi maka keamanan jaringan tersebut akan mudah untuk di tembus oleh pihak-pihak yang tidak berkepentingan (unauthorized user). Sekali seorang "sniffer" berhasil mendapatkan informasi SSID sebuah access point, maka "sniffer" tersebut dapat memotret lalu lintas dalam jaringan wireless tersebut dan membuka informasi tentang semua hal dalam jaringan tersebut, seperti user name dan password. Ketika seorang sniffer berhasil melakukan pengamatan/ observasi dan menggunakan informasi yang didapat tersebut untuk masuk kedalam jaringan dan mengakses atau menggunakan sumber daya didalam sistem tersebut tanpa ijin, maka pada tahapan ini serangan pasif (passive attack) berubah menjadi jenis serangan aktif (active attack).

Untuk melindungi jaringan wireless terhadap program-program komputer yang mampu mengeteksi keberadaan sinyal jaringan wireless, maka seorang pengelola jaringan wireless (administrator) harus melakukan konfigurasi ulang terhadap semua konfigurasi dasar dari perangkat jaringan wireless tersebut jika konfigurasinya masih menggunakan konfigurasi standar/ default yang diberikan oleh vendor pembuat perangkat jaringan wireless tersebut ketika perangkat tersebut pertama kali dibeli. Diantaranya adalah

dengan menerapkan sistem keamanan tertutup yaitu dengan cara melakukan konfigurasi agar sebuah Access Point tidak dapat merespon permintaan koneksi (request) terhadap status SSID-nya yang biasanya diminta oleh program-program seperti NetStumbler. Melalui cara ini sebuah access point dalam sebuah jaringan wireless tetap tidak dapat di deteksi (invisible) oleh pihak-pihak yang tidak berhak untuk mengakses jaringan wireless tersebut.

Saat ini kebanyakan perangkat access point untuk jaringan wireless sangat mudah untuk konfigurasinya dengan tujuan untuk memudahkan penggunanya dan menggunakan jaringan tersebut. Namun dengan segala kemudahan tersebut ternyata memiliki kelemahan juga. Demi mengutamakan kemudahan konfigurasi, maka beberapa vendor pembuat access point tidak memberikan sentuhan aspek keamanan pada konfigurasi dasar yang diberikan pada access point yang mereka produksi. Hal ini disebabkan karena untuk melakukan konfigurasi terhadap keamanan jaringan didalam sebuah perangkat access point cukup rumit dan harus mempertimbangkan banyak aspek. Sehingga jika keamanan jaringan dimasukkan kedalam konfigurasi dasar perangkat access point tentunya prosesnya tidak mudah lagi dan membutuhkan keahlian khusus dari user.

Berikut ini beberapa hal dasar yang dapat dilakukan untuk melindungi jaringan wireless dari serangan pasif maupun serangan aktif:

1. Amankan Router wireless atau Antarmuka Halaman Administrator Access Point.

   Hampir semua router dan access point memiliki password untuk administrator yang dibutuhkan pada saat login kedalam perangkat wireless dan untuk melakukan pengaturan konfigurasi didalam perangkat access point. Kebanyakan perangkat access point menggunakan password default yang sangat sederhana dan tidak aman. Misalnya password dengan kata kunci “password” juga atau menggunakan kata kunci nama perusahaannya, dan beberapa bahkan tidak memiliki password sama sekali. Untuk kasus seperti ini, langkah pertama yang dilakukan oleh seorang administrator

ketika melakukan pengaturan pertama kali terhadap perangkat router wireless atau access point adalah dengan mengganti password default pada perangkat tersebut dengan password lain yang lebih aman. Karena password ini jarang sekali digunakan karena untuk melakukan konfigurasi terhadap perangkat access point biasanya sangat jarang dilakukan, maka gunakanlah password yang mudah untuk diingat tetapi sulit untuk ditebak atau dapat juga dengan cara menuliskan password tersebut agar tidak mudah lupa tetapi disimpan di tempat yang aman jika passsword tersebut memang harus dituliskan agar tidak lupa. Jika akhirnya password tersebut dilupakan maka satu-satunya cara adalah dengan cara melakukan reset terhadap perangkat access point tersebut sehingga semua konfigurasinya dikembalikan ke konfigurasi default seperti semula ketika perangkat wireless tersebut pertama kali dibeli dari vendor. Sehingga administrator harus melakukan konfigurasi ulang terhadap perangkat wireless tersebut untuk aspek keamanannya.

Berikut adalah beberapa trik untuk membuat password yang relatif aman:

- password jangan menggunakan informasi pribadi seperti nama, tanggal lahir.
- password harus mudah diingat tapi sulit untuk ditebak.
- gunakanlah password yang berbeda untuk mengakses sistem yang berbeda.
- gantilah password secara berkala untuk menghindari serangan terhadap password menggunakan program “password cracking”.
- jika password harus dituliskan dan disimpan dalam sebuah file komputer karena sulit untuk diingat maka simpanlah ditempat yang aman dan file tersebut di enkripsi.

2. Jangan Melakukan Broadcast terhadap SSID access point.

   Kebanyakan access point dan router secara otomatis melakukan proses broadcast untuk nama jaringan, atau SSID (Service Set IDentifier). Pengaturan ini tentu saja memudahkan pengaturan

jaringan wireless pada client dan membuat perangkat access point dapat terlihat oleh semua sistem jaringan wireless yang masuk dalam jangkauan sinyal perangkat access point tersebut. Sehingga dengan mengaktifkan SSID pada access point tersebut memungkinkan semua pihak untuk mendeteksi kehadiran dari jaringan access point tersebut baik oleh pihak yang berhak maupun oleh pihak yang tidak berhak untuk mengakses jaringan tersebut. Hal ini tentu saja dapat menimbulkan celah keamanan pada jaringan wireless tersebut. Untuk mengamankan maka sebaiknya fitur SSID broadcast di matikan sehingga jaringan wireless tersebut menjadi tidak terlihat (invisible) oleh user-user lain yang tidak berhak dan tidak terdaftar didalam jaringan wireless tersebut. Bagi user awam hal ini tidak dapat di deteksi tetapi bagi seorang "sniffer" tentunya cara ini tidak berpengaruh karena dengan menggunakan program-program komputer tertentu seperti NetStumbler para "sniffer" masih dapat mendeteksi keberadaan perangkat access point untuk jaringan wireless tersebut.

Aktifkan Fitur Keamanan Enkripsi WPA daripada WEP.

Fitur keamaanan enkripsi WEP (Wired Equipment Privacy) yang selama ini banyak di terapkan pada perangkat access point telah diketahui memiliki banyak kelemahan sehingga relatif mudah bagi seseorang untuk membuka kode-kode enkripsinya dan mengakses jaringan wireless hanya dengan menggunakan perangkat yang tepat. Cara yang lebih baik untuk melindungi jaringan wireless saat ini adalah dengan menggunakan WPA (Wi-Fi Protected Access). WPA menyediakan lebih banyak fitur keamanan dan kemudahan dalam penggunaannya, tidak seperti pada WEP yang membatasi penggunaan karakter password hanya pada angka 0-9 dan huruf mulai A-F. Dukungan terhadap WPA sudah disertakan pada sistem operasi windows XP (dengan service pack terbaru) dan secara virtual pada perangkat jaringan wireless terbaru saat ini dan pada sistem operasi. Versi WPA terbaru saat ini adalah WPA2 yang dapat ditemukan pada perangkat jaringan wireless terbaru saat ini dan menyediakan mekanisme enkripsi yang lebih baik. Namun

untuk menggunakan fitur WPA2 ini mungkin saja harus mendownload patch terbaru pada sistem operasi windows XP. Karena fitur ini relatif baru dan belum semua sistem operasi windows XP mendukung penggunaannya.

Gambar 3. Penggunaan enkripsi WEP dan WPA dalam pengamanan jaringan wireless

4. Gunakanlah WEP daripada tidak menggunakan sama sekali.
   Jika ternyata ada beberapa perangkat wireless yang beredar di pasaran saat ini hanya mendukung enkripsi WEP (biasanya ditemukan pada perangkat yang berbasis non-PC seperti media player, PDA, dan DVR), maka gunakanlah fitur enkripsi WEP walaupun relatif tidak aman daripada tidak sama sekali dan gunakanlah kunci yang sulit untuk ditebak.
5. Gunakan penyaringan terhadap kontrol akses ke jaringan wireless dengan menggunakan penyaringan MAC.
   Tidak seperti penggunaan alamat IP, alamat MAC sifatnya unik untuk membedakan antara satu perangkat jaringan yang satu dengan yang lainnya. Sehingga dengan mengaktifkan fitur

penyaringan menggunakan MAC maka dapat dibatasi akses ke dalam jaringan wireless oleh hanya pihak yang alamat MAC-nya sudah terdaftar didalam perangkat access point tersebut. Untuk mendaftarkan alamat MAC setiap pengguna didalam jaringan wireless maka harus diketahui terlebih dahulu 12 karakter alamat MAC yang terdapat pada masing-masing perangkat jaringan yang akan melakukan koneksi ke perangkat access point. Tentunya cara ini sedikit tidak nyaman dan tidak fleksibel karena seorang administrator harus mendaftarkan semua alamat MAC untuk setiap user/ client yang akan terhubung kedalam jaringan tersebut. Jika jumlah client pengguna jaringan wireless tersebut banyak tentu saja merepotkan seorang administratori jaringan. Saat ini sudah banyak program yang termasuk kategori "hacking tool" yang dapat digunakan untuk melakukan pemalsuan/ "spoofing" terhadap alamat MAC. Sehingga diperlukan perhatian yang cukup teliti dari seorang administrator jaringan wireless untuk mengetahui mana alamat MAC yang sah dan mana alamat MAC yang palsu. Sehingga dengan memalsukan/ spoofing alamat MAC sesuai dengan alamat MAC yang terdaftar didalam jaringan wireless tersebut maka pihak yang tidak berhak dapat masuk dan mengakses jaringan wireless tersebut.

6. Mengurangi kekuatan pancaran perangkat wireless (access point). Fitur ini sebenarnya tidak terdapat di semua router wireless dan access point, tetapi ada beberapa yang perangkat wireless yang menyediakan fitur untuk menurunkan kekuatan perangkat wireless dalam memancarkan sinyalnya sehingga jangkauan sinyalnya semakin sempit. Walaupun tidak selamanya mungkin untuk melakukan proses pengaturan secara tepat untuk ukuran sinyalnya namun cara ini tetap saja berhasil untuk mengurangi potensi timbulnya celah keamanan pada sistem jaringan wireless dan meminimalkan peluang pihak diluar sistem yang tidak berhak untuk mengakses perangkat jaringan wireless tersebut.
7. Matikan fitur/ layanan administrasi jarak jauh.

Hampir semua perangkat router wireless menyediakan fitur untuk dapat dikelola secara jarak jauh melalui jaringan internet. idealnya, penggunaan fitur ini hanya pada saat penentuan alamat IP tertentu atau untuk membatasi jangkauan penggunaan alamat IP yang boleh mengakses perangkat router tersebut. selain untuk dua kegiatan tersebut diatas, sebaiknya fitur ini dimatikan. karena dengan mengaktifkan fitur ini maka setiap orang yang berada dalam jangkauan sinyal perangkat router wireless tersebut berpotensi untuk menemukan dan mengakses perangkat router wireless tersebut. Sehingga selalu matikan fitur ini sebagai suatu kebijakan dalam pengelolaan perangkat router didalam sebuah jaringan wireless. Sehingga seorang administrator tidak dapat melakukan pengelolaan jaringan wirelessnya secara remote via internet. Biasanya fitur ini secara default dimatikan oleh vendor pembuat perangkat router tersebut ketika pertama kali dibeli untuk alasan keamanan. Namun tidak ada salahnya untuk melakukan pengecekan secara berkala terhadap fitur ini didalam perangkat jaringan wireless apakah benar sudah di non-aktifkan atau masih aktif.

Penutup

Jaringan wireless merupakan jaringan komputer yang sangat terbuka dan rentan terhadap celah keamanan. Hal ini disebabkan oleh komponen-komponen penyusun jaringan ini yang secara fisik sangat sulit untuk diamankan. Berbeda dengan jaringan berbasis kabel yang pengamanan fisiknya mudah untuk di amankan dan di kendalikan, jaringan berbasis wireless sangat sulit untuk dikendalikan. Pemancaran sinyal frekuensi yang digunakan oleh perangkat wireless memungkinkan semua pihak dapat mendeteksi dan mengakses jaringan ini selama menggunakan perangkat wireless penerima yang kompatibel dan sinyalnya dapat dijangkau.

Saat ini banyak sekali jenis-jenis program komputer yang dapat digunakan untuk melakukan serangan terhadap jaringan wireless, baik jenis serangan pasif yang sifatnya tidak merusak dan

hanya mencuri informasi sampai ke jenis serangan aktif yang dapat merusak sistem dan menggunakan semua sumber daya yang terdapat dalam jaringan wireless tersebut. Karena karakteristik perangkat wireless yang sulit untuk diamankan secara fisik maka pengamanannya hanya dapat dilakukan dengan menggunakan kebijakan atau menggunakan program komputer yang biasanya disediakan oleh vendor pembuat perangkat wireless tersebut dengan hanya melakukan pengaturan sederhana dan mudah.

Daftar Pustaka

CompTIA Security+, Part 1 – security concepts., www.comptia.net
Network Security Essentials., Stalling W., Prentice Hall., 2004
http://www.more.net –Network Auditing-, 2007.