

IIS server sering berada dalam bahaya karena banyak senjata yang didesain untuk menyerang produk Microsoft. Mengetahui hal itu, administrator harus siap untuk mengimplementasikan beragam tingkat keamanan.

Gunung Sarjono



Bagaimana Mengamankan IIS Web Server?

► Biasanya, suatu situs web didesain untuk memberikan akses ke informasi dengan cara yang paling mudah. Namun dalam beberapa tahun terakhir, masalah keamanan yang disebabkan oleh meningkatnya serangan *hacker*, virus, dan *worm* telah menghilangkan kemudahan. Microsoft Internet Information Services (IIS) Web Server secara khusus sering diserang, walaupun Apache Web Server juga target yang populer.

Oleh karena itu, kami hendak mencoba memberikan bagaimana Anda mengamankan IIS Web Server dengan anggaran yang pas-pasan. Meskipun begitu, cara yang diberikan di sini juga dapat digunakan oleh Anda yang mempunyai anggaran yang besar.

Update Windows

Menggunakan *update* dan *security patch* terbaru merupakan langkah pengamanan yang paling mudah dilakukan. *download update* ke suatu komputer khusus pada jaringan dan berikan update

ke web server dari komputer tersebut. Dengan melakukan itu, Anda dapat mencegah web server untuk *browsing* Internet secara langsung.

Hapus Web Site Default

Banyak penyerang mengincar folder *inetpub* untuk meletakkan “barangnya” yang dapat membuat server Anda berhenti. Salah satu cara untuk mencegah serangan semacam ini adalah dengan *men-disable Web site default* yang terinstal bersama IIS. Selanjutnya, pada waktu *surfer* mencoba untuk mengakses situs web Anda dengan alamat IP, *request* tersebut akan hilang. Pindahkan situs web Anda yang sebenarnya ke folder pada partisi lain dengan NTFS permission.

Uninstall FTP dan SMTP Jika Anda Tidak Menggunakannya

Cara paling mudah untuk masuk ke dalam komputer adalah melalui FTP. FTP didesain untuk akses baca/tulis yang mudah, dan

jika Anda menggunakan otentikasi, *username* dan *password* Anda akan dikirim melalui Internet dalam teks murni. SMTP juga merupakan layanan yang memberikan akses tulis ke folder-nya. Dengan *men-disable* kedua *service* tersebut, Anda akan menghilangkan kesempatan *hacker* untuk bersenang-senang.

Periksa Grup Administrator dan Catat Service Secara Teratur

Pernah suatu ketika kami menemukan *user* baru dalam grup Administrator. Pada waktu seseorang telah masuk sejauh ini ke sistem Anda, ia biasanya menaruh beberapa bom waktu yang pada akhirnya menghancurkan sistem Anda atau mengambil semua *bandwidth* untuk keperluan sang *hacker*. Jika ini terjadi, mungkin sudah terlambat untuk melakukan apapun selain memformat harddisk Anda dan mengembalikan datanya dari *back-up* yang Anda buat setiap harinya. Catatlah *service* pada IIS server secara teratur (harian/mingguan)

dan pastikan seminimal mungkin yang berjalan. Anda harus mengingat apa yang ada di sini.

Windows 2000 Resource Kit mempunyai utility bernama tlist.exe yang mencatat service yang berjalan di bawah svchost. Pada waktu menjalankan utility ini, Anda mungkin akan menemukan service tersembunyi yang perlu Anda ketahui. Berikut adalah satu petunjuk: service apapun dengan kata “daemon” pada namanya mungkin bukan asli dari Windows dan tidak boleh berada pada IIS server.

Atur Hak Tulis ke Server

Ini kedengarannya sederhana, tetapi pada kampus, web server mempunyai banyak “pemilik”. Anggota fakultas ingin informasi ruang kelas dapat diakses oleh murid yang jauh. Anggota staf ini berbagi informasi kerja dengan pegawai yang lain.

Hal ini dapat menjadi mimpi buruk bagi setiap folder pada server. Salah satu cara untuk mengatasinya adalah dengan menginstal server kedua khusus untuk *share* dan penyimpanan. Kemudian konfigurasi web server Anda untuk menunjuk ke folder pada share server. Dengan langkah ini, administrator dapat membatasi akses tulis ke web server itu sendiri khusus untuk grup administrator.

Gunakan Password yang Kompleks

Kami menemukan bukti pada *Event Viewer* akan kemungkinan adanya *hacker*. Ia telah masuk cukup jauh untuk menjalankan program pembobol *password* untuk setiap *user domain*. Jika ada *user* dengan password yang lemah (seperti “password” atau “changeme” atau kata dalam kamus), maka *hacker* ini akan dengan cepat dan mudah mendapatkan akses ke *account user* tersebut.

Kurangi/Hilangkan Share pada Web Server

Jika hanya administrator yang mempunyai hak tulis ke *web server*, maka tidak ada alasan untuk membuat *share*. *Share* merupakan hal yang sangat menarik bagi penyerang. Dengan menjalankan *batch file* sederhana secara berulang-ulang, seorang *hacker* bisa mendapatkan alamat IP untuk *share* yang terbuka untuk *Everyone/Full Control*.

Disable NetBIOS over TCP/IP

Ini merupakan hal yang sulit. Banyak pemilik yang ingin mengakses *web server* dengan UNC pathname. Dengan di-*disable*-nya NetBIOS, mereka tidak akan bisa lagi melakukan itu. Sementara di lain pihak, jika NetBIOS di-*disable*, *hacker* tidak akan bisa melihat resource pada LAN Anda. Ada suatu timbal-balik. Jika administrator mengimplementasi hal ini, maka langkah selanjutnya adalah mengedukasi pembuat web tentang bagaimana mem-*publish* web tanpa NetBIOS.

Gunakan TCP Port Blocking

Ini juga merupakan *tool* yang sulit. Jika Anda tahu dengan pasti setiap port TCP yang digunakan untuk mengakses server, maka Anda dapat membuka *properties* kartu jaringan yang terikat (*binding*) dengan TCP/IP dan blokir semua port kecuali yang Anda butuhkan.

Namun, gunakan tool ini dengan hati-hati, karena Anda tentu tidak ingin mengunci diri sendiri dari web server, terutama jika Anda mengaksesnya secara *remote*. Untuk daftar terbaru tentang port TCP buka <http://www.iana.org/assignments/port-numbers>.

Cek File *.bat dan *.exe Secara Teratur

Satu kali seminggu periksalah file *.bat dan *.exe untuk melihat apakah ada file *executable* pada web server yang dapat menjadi sasaran empuk *hacker* dan mimpi buruk Anda. Di samping file-file tersebut, periksa juga file *.reg. Jika Anda mengklik kanan dan memilih “edit”, maka akan melihat modifikasi apa yang telah dilakukan di registry yang memungkinkan *hacker* mengakses *resource* sistem Anda.

Atur Sekuriti Direktori IIS

Direktori IIS memungkinkan Anda menolak alamat IP, subnet, atau bahkan nama *domain* tertentu. Sebagai alternatif, Anda dapat menggunakan tool bernama *WhosOn*, yang dapat memberitahu alamat IP yang mengakses file pada server. *WhosOn* memberi daftar “*Exceptions*”, yaitu hal-hal yang perlu diselidiki lebih lanjut, untuk berbagai macam alasan, *browser* dicurigai.

Pada waktu Anda menemukan seseorang mencoba untuk, misalnya, mengakses cmd.exe, maka Anda dapat—selagi Anda dalam program—mencegah user tersebut menggunakan web server lebih lanjut. Namun tentu saja, pada situs web yang sibuk, ini bisa memakan waktu berjam-jam!

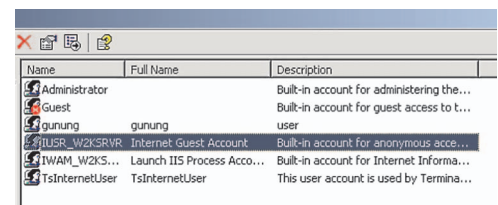
Perlu diingat bahwa kinerja server akan terpengaruh pada waktu Anda menggunakan tool tersebut, terutama jika Anda menolak keseluruhan nama domain. Ini karena resolusi nama harus dilakukan kepada semua pengunjung untuk memastikan bahwa user tersebut bukan anggota domain yang ditolak.

Gunakan Sekuriti NTFS

Secara *default*, drive NTFS terbuka untuk *Everyone/Full Control* sampai Anda mengunci mereka. Namun, jangan sampai Anda mengunci diri sendiri. Semua orang tidak boleh diberi akses apapun. Administrator butuh *full control*, *account backdoor* admin (jika Anda punya) butuh full control, dan *System* dan *Services* masing-masing membutuhkan akses, bergantung kepada tiap file. Folder yang paling penting adalah System32, dan *permission* pada folder ini haruslah seminim mungkin. Dengan menggunakan NTFS permission pada web server, dapat membantu mengunci file dan aplikasi yang tidak boleh diakses oleh *web surfer*.

Atur User Account

Setelah menginstal IIS, Anda mungkin mempunyai *account* bernama IUSR. *Disable* account ini, kecuali jika Anda benar-benar membutuhkannya. User ini mudah disusupi dan merupakan sasaran besar bagi *hacker*. Untuk membantu mengatur user account, pastikan *security policy* lokal seketat mungkin. IUSR sedapat mungkin mempunyai akses yang minim. ■



Name	Full Name	Description
Administrator	Administrator	Built-in account for administering the...
Guest	Guest	Built-in account for guest access to t...
gunung	gunung	user
IUSR_W2KSRVR	Internet Guest Account	Built-in account for anonymous acce...
IWAM_W2KS...	Launch IIS Process Acco...	Built-in account for Internet Informa...
TsInternetUser	TsInternetUser	This user account is used by Termina...

Internet Guest Account disable IUSR untuk mengamankan IIS server.

Kontrol dan kenali jaringan rumah Anda yang sederhana dengan baik, maka semua masalah dapat dideteksi. Tidak ada lagi kejadian-kejadian yang Anda anggap gaib di dalamnya. Jaringan Anda akan bekerja efektif dan efisien untuk Anda.

Hayri



Menjadi Penguasa Jaringan Rumah Anda

► Jaringan komunikasi data sebenarnya adalah sebuah rimba belantara yang lebat dan pekat. Penuh dengan berbagai pernak-pernik yang membingungkan dan terlebih lagi pernak-pernik ini banyak yang tidak kasat mata. Apa yang terjadi ketika ada sesuatu yang perlu Anda cari di tengah-tengah rimba belantara? Seperti mencari jarum dalam tumpukan jerami, bukan?

Begitu juga dengan jaringan komputer, ketika Anda ingin mencari sesuatu di dalamnya, akan sangat susah jika Anda hanya mengandalkan mata biasa. Melakukan *troubleshooting* suatu masalah yang terjadi di jaringan Anda misalnya, merupakan suatu pekerjaan yang amat sulit jika dilakukan tanpa bantuan apa-apa. Untuk itu, sebuah jaringan yang baik haruslah dapat dikenali, dimengerti, dan dilihat dengan mudah isinya. Jaringan yang baik haruslah memiliki manajemen yang baik, tidak hanya sekedar performanya saja yang hebat.

Memanajemi sebuah jaringan rumah sederhana menjadi tidaklah sulit jika Anda mengetahui data apa saja yang perlu dikumpulkan dari jaringan, apa saja yang perlu diatur dalam jaringan, dan apa saja yang perlu dihilangkan dari jaringan Anda. Berikut ini adalah beberapa langkah manajemen yang penting yang perlu Anda kenali, pelajari, dan terapkan pada jaringan rumah Anda untuk selangkah lebih teratur.

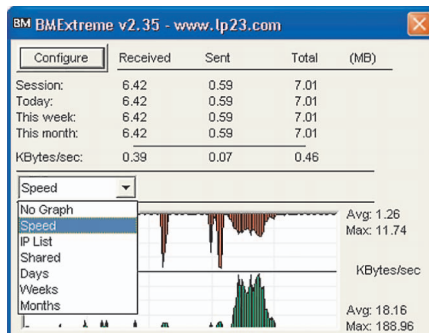
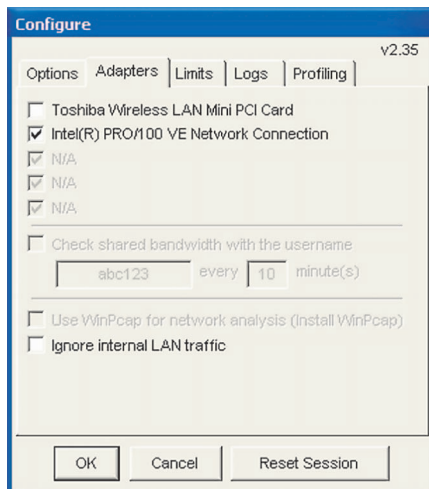
Traffic Monitoring

Melakukan monitoring terhadap lalu-lintas data Anda di jaringan merupakan hal yang paling utama dan penting yang harus dilakukan oleh seorang administrator jaringan untuk benar-benar menguasai jaringannya. Dengan mendapatkan gambaran yang jelas mengenai *traffic* yang ada dalam jaringan Anda, banyak sekali manfaat yang bisa didapatkan. Dengan melakukan monitoring *traffic*, hasilnya dapat Anda gunakan untuk keperluan *troubleshooting*,

keperluan *maintenance*, keperluan penelitian karakteristik jaringan Anda, keperluan pemantauan keamanan jaringan, memantau virus, dan banyak lagi manfaatnya.

Terlebih lagi jika jaringan Anda terkoneksi ke Internet, monitoring *traffic* merupakan suatu keharusan jika Anda tidak ingin uang Anda sia-sia terbuang. *Traffic* penggunaan Internet broadband Anda misalnya, tentu akan sangat berguna untuk dimonitor bagaimana tren penggunaan koneksi Internet Anda. Dengan memonitoring *traffic*, adalah langkah awal untuk mengenal lebih dalam mengenai jaringan Anda.

Untuk melakukan monitoring *traffic*, pertama-tama Anda harus menentukan titik mana yang merupakan pusat dari aktivitas jaringan Anda. Jika Anda melakukan *sharing* Internet dalam jaringan, yang menjadi titik pusat jaringan adalah pada sebuah server yang memiliki tugas melakukan *sharing* Internet. Pada server inilah, tempat



Anda harus menentukan dulu interface mana yang penting untuk dimonitor. Selanjutnya tinggal pantau saja dengan menggunakan BMExtreme.

yang paling tepat untuk memasang mata-mata jaringan Anda. Traffic yang keluar dan masuk pada titik ini akan cukup mewakili besarnya penggunaan Internet pada jaringan Anda.

Untuk memonitor jaringan rumah yang sederhana dengan jumlah pengguna yang tidak terlalu banyak dan topologi jaringan yang tidak terlalu kompleks, salah satu aplikasi yang dapat Anda gunakan untuk ini adalah BMExtreme. Program yang bisa Anda dapatkan dengan gratis versi trialnya ini di situs www.lp23.com, memiliki kemampuan monitoring sederhana dan ringan namun cukup berguna dalam memantau jaringan rumah Anda. Anda dapat mengatur interface mana yang ingin Anda monitor, apakah port Ethernet Anda atau interface wireless jika ada. Sebaiknya kali pertama menggunakan program ini, tentukan lebih dulu interface mana yang penting untuk Anda ambil datanya.

Setelah menentukan interface mana yang dimonitor, Anda dapat langsung

melihat grafik dan statistiknya pada halaman pertama dari program ini. Anda dapat menentukan apakah ingin melihat angka-angka statistiknya saja ataupun berikut grafiknya.

Tampilan grafik dapat Anda atur jangka waktunya untuk melakukan refresh tampilan, apakah setiap 5 menit, 30 menit-an, 1 jam-an, dan masih banyak lagi pilihan waktunya. Anda akan melihat tampilan grafik yang berbeda-beda jika Anda mengatur waktu ini. Selain itu, ada juga informasi mengenai IP berapa saja yang telah melakukan koneksi dengan interface tersebut. Informasi ini sangat berguna untuk mendeteksi alamat-alamat IP berapa saja yang paling sering Anda tuju.

Yang menarik dari program BMExtreme ini adalah tersedianya tab *Limits* yang isinya merupakan fasilitas pembatasan *bandwidth* untuk sebuah interface. Anda dapat membatasi berapa besar total data yang keluar dan masuk pada interface yang Anda inginkan. Jika batas tersebut lewat, maka interface tersebut tidak akan melayani lagi komunikasi Anda.

Selain itu, ada pula fasilitas *Profiling* yang memungkinkan Anda membuat *profile* untuk monitoring. Misalnya, Anda hanya ingin memonitor traffic yang keluar-masuk menggunakan port 80 pada interface wireless, Anda bisa langsung membuatnya di sini. Jika profil diaktifkan, maka yang terlihat pada grafik adalah data mengenai apa yang telah ditentukan di profil ini.

Dengan menggunakan program semacam ini, jaringan Anda bisa lebih terpantau dengan baik. Anda bisa segera mengetahui apabila bandwidth Internet Anda telah mencapai batas maksimal. Atau Anda akan segera mengetahui ketika Anda serangan dari luar terhadap jaringan Anda. Atau ada virus yang berusaha memenuhi jaringan Anda juga bisa dideteksi. Semua itu tersedia dalam program yang kecil dan tidak akan memakan banyak *resource* komputer Anda seperti program-program monitoring besar lainnya.

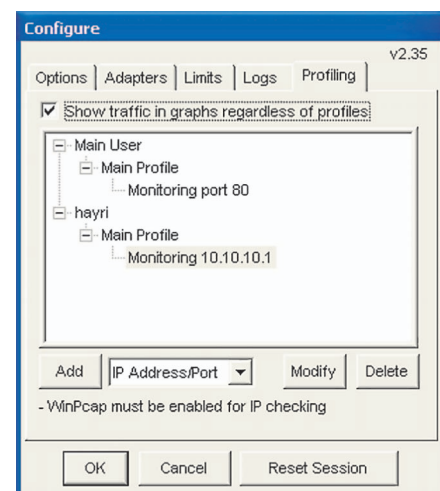
Bandwidth Manager

Bandwidth, khususnya bandwidth Internet masih merupakan barang mewah di negara kita. Harganya yang masih

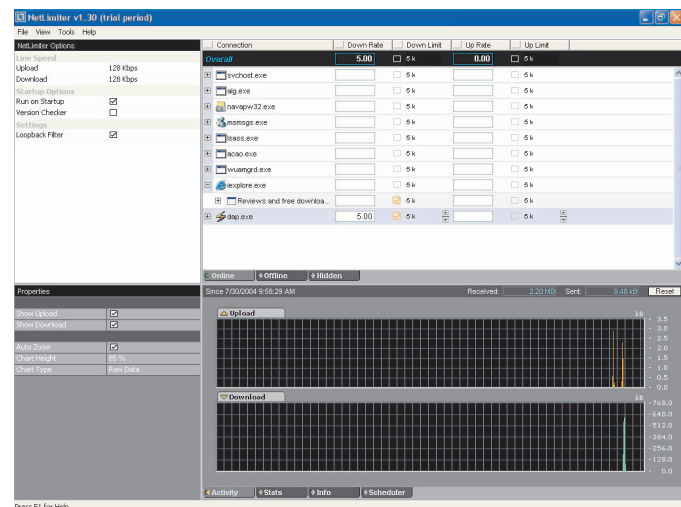
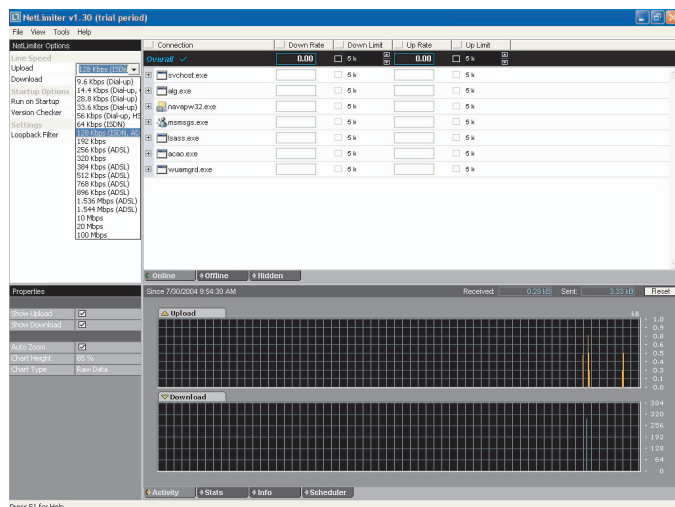
tergolong mahal membuat para pengguna jarang yang bisa memilikinya dalam jumlah banyak. Malah sering kali ukurannya kurang jauh dari kebutuhan yang sebenarnya. Maka dari itu, sangatlah disayangkan jika ada penggunaan bandwidth Internet yang tidak efisien. Sampah-sampah elektronik seperti virus, *spam*, *adware*, dan banyak lagi merupakan salah satu pendukung penggunaan bandwidth yang tidak efisien.

Namun selain itu, ketimpangan-ketimpangan penggunaan bandwidth juga sering terjadi. Ketika ada salah satu pengguna di dalam jaringan melakukan proses *download* besar-besaran, maka pengguna lain bisa saja tidak kebagian jatah bandwidth. Akibat dari ini adalah para pengguna lain tidak lancar berkomunikasi ke Internet. Hal ini akan menyebabkan pengguna merasa lambat dalam melakukan *browsing*, *chatting*, *download*, atau bahkan tidak bisa sama sekali.

Untuk menguasai jaringan dari masalah seperti ini, Anda memerlukan sebuah program yang memiliki kemampuan mengatur besar kecilnya bandwidth yang digunakan oleh seseorang atau sebuah program Internet tertentu. Program jenis ini biasanya sering disebut dengan istilah *bandwidth manager*. Bandwidth manager memiliki tugas utama untuk memamanajemeni bandwidth yang ada agar lebih teratur dan efisien. Salah satu program bandwidth manager yang



Fasilitas profiling dari BMExtreme dapat memberikan Anda informasi mengenai traffic sebuah servis tertentu.



Bandwidth manager sederhana ini terbilang cukup hebat untuk skala jaringan rumah dan kantor kecil. Menentukan batasan-batasan bandwidth per program juga bisa dilakukannya dengan sangat akurat.

sederhana namun cukup berkualitas adalah Netlimiter.

Netlimiter merupakan program bandwidth manager sederhana yang penggunaannya cocok untuk di dalam LAN atau jaringan yang tidak terlalu besar ukurannya. Program Netlimiter atau yang sejenis ini biasanya diinstal pada server Internet sharing agar semua proses komunikasi Internet tertangkap oleh program ini. Setelah tertangkap, Anda baru bisa mengatur besarnya bandwidth yang akan digunakan untuk sebuah proses komunikasi Internet tersebut. Biasanya semua proses komunikasi Internet pasti akan masuk ke dalam program ini tanpa kecuali.

Setelah tampil di menu pengaturannya, Anda dapat dengan bebas mengatur berapa besar bandwidth yang keluar dan berapa besar yang masuk. Besarnya parameter ini juga tidak harus simetris, jadi boleh berlainan sesuai dengan kebutuhan Anda. Program ini terbilang cukup hebat karena berapa pun besarnya nilai limit yang ditentukan untuk suatu program, maka segitulah besarnya bandwidth yang akan diberikan kepada sebuah koneksi. Jadi, pengaturannya benar-benar akurat dan tepat.

Selain pengaturan bandwidth, disediakan juga grafik-grafik monitoring traffic yang saat itu sedang berlangsung. Ini merupakan sebuah nilai plus untuk program ini. Anda dapat mengatur bandwidth sambil memonitornya me-

lalui bentuk grafik. Jaringan Anda kini sudah lebih Anda kuasai lagi.

Firewall

Tembok api penghadang semua gangguan juga amat sangat penting perannya dalam menjaga jaringan rumah Anda agar tetap dapat berjalan dengan baik. Menguasai lebih dulu jaringan Anda sebelum orang lain menguasainya, tentu merupakan tindakan bijaksana. Jika jaringan rumah Anda tidak dikuasai dengan baik, berbagai macam *backdoor*, program pengintai, *adware*, dan banyak lagi, tentu akan segera masuk. Untuk itu, tangkislah semua usaha pengacau dengan menginstal *firewall* pada jaringan Anda.

Firewall sebenarnya merupakan sekumpulan peraturan yang dibuat untuk mengatur data yang keluar dan masuk ke dalam dan dari interface-interface jaringan Anda. Sekumpulan aturan tersebut dibuat sedemikian rupa sehingga proses-proses komunikasi yang tidak diinginkan, dari luar maupun dari dalam, bisa diblok agar tidak sampai ke tujuannya. Sedangkan komunikasi yang diinginkan tetap dapat diteruskan.

Yang penting untuk diperhatikan dalam membuat sistem firewall dalam jaringan rumah Anda adalah penyusunan peraturan dan peletakkannya. Penyusunan peraturan yang baik tentu hasilnya akan memudahkan dan membuat jari-

ngan Anda aman. Sebaliknya peraturan yang tidak dibuat dengan benar akan sangat menyusahkan Anda. Karena selain tidak aman, komunikasi Anda keluar masuk bisa kacau.

Komunikasi yang seharusnya Anda inginkan, malah terblokir oleh sistem firewall Anda. Sebaliknya sebuah komunikasi yang harusnya tidak boleh terbuka ke dalam jaringan pribadi, malah terbuka selebar-lebarnya. Semua ini bisa dikarenakan program firewall yang kurang hebat, pendesainan peraturan yang tidak baik, kesalahan konfigurasi, ketidaksengajaan, dan banyak lagi.

Untuk itu, penting sekali untuk menentukan program firewall apa yang akan digunakan dalam jaringan rumah Anda. Salah satu program yang banyak dipuji-puji oleh para pengguna komputer adalah Zone Alarm. Selain tersedia versi komersilnya, tersedia pula versi gratisnya yang bebas Anda *download* dan gunakan. Namun dengan kemampuan yang masih terbatas tentunya. Anda dapat mendownload-nya di www.zonelabs.com, atau dapat juga menemukannya di CD *PC Media* edisi ini. Meski tidak sehebat dan selengkap versi komersilnya, program gratisnya ini sudah cukup untuk melindungi jaringan rumah sederhana Anda.

Menggunakan Zone Alarm Anda akan mendapatkan empat buah fitur yang berkonsentrasi untuk melindungi perangkat komputer. Fitur pertama adalah *Firewall* yang bertugas untuk memblokir dan melewatkan sebuah proses komu-

nikasi. *Firewall Zone Alarm* membagi-bagi daerah kerjanya dengan sebutan *Zone*, *Internet Zone* dan *Trusted Zone*.

Zone-zone ini dapat Anda atur sendiri tingkat keamanannya. *High* untuk tingkat pengamanan yang tinggi, *Medium* yang sedang, dan *Low* yang rendah. Di setiap tingkat pengamanan terdapat seperangkat peraturan yang bertugas membatasi proses komunikasi agar tidak terlalu bebas.

Pada versi gratisnya ini, Anda hanya dapat menentukan akan menggunakan tingkat pengamanan yang mana, tanpa dapat mengetahui apa dan bagaimana isi peraturan-peraturan di dalamnya. Membuat peraturan sendiri lebih tidak mungkin lagi. Yang masih dapat Anda atur hanyalah menggolongkan alamat-alamat IP atau segmen-segmen jaringan mana saja yang termasuk dalam *Trusted zone* atau *Internet zone*. Meski demikian, firewall ini menjalankan fungsinya dengan cukup baik.

Fitur lainnya adalah *Program Control*, yang banyak mengatur komunikasi ke luar dari program-program yang terinstal di komputer Anda. Program yang Anda instal di komputer terkadang perlu juga terkoneksi ke Internet untuk sekadar melakukan *update* maupun melakukan tugas utamanya. Dengan fasilitas ini, komunikasi yang ingin dibangun oleh program-program tersebut juga dapat dikontrol oleh *Zone Alarm*. Program yang tidak sesuai dengan kriteria *Zone Alarm* tidak akan dilewatkan karena dianggap membahayakan keamanan perangkat komputer Anda. Namun, tingkat keamanan ini juga dapat diatur.

Antivirus *Monitoring* juga disediakan di sini. Fitur ini bertugas memonitor program antivirus yang terinstal di komputer Anda apakah bekerja dengan baik dan selalu *up-to-date* atau tidak. Program-program antivirus yang terinstal akan segera terdeteksi oleh *Zone Alarm*. Setelah itu, Anda dapat mengetahui antivirus mana yang tidak *up-to-date* *virus list*-nya atau yang sudah *expired* waktu instalasinya, dan banyak lagi.

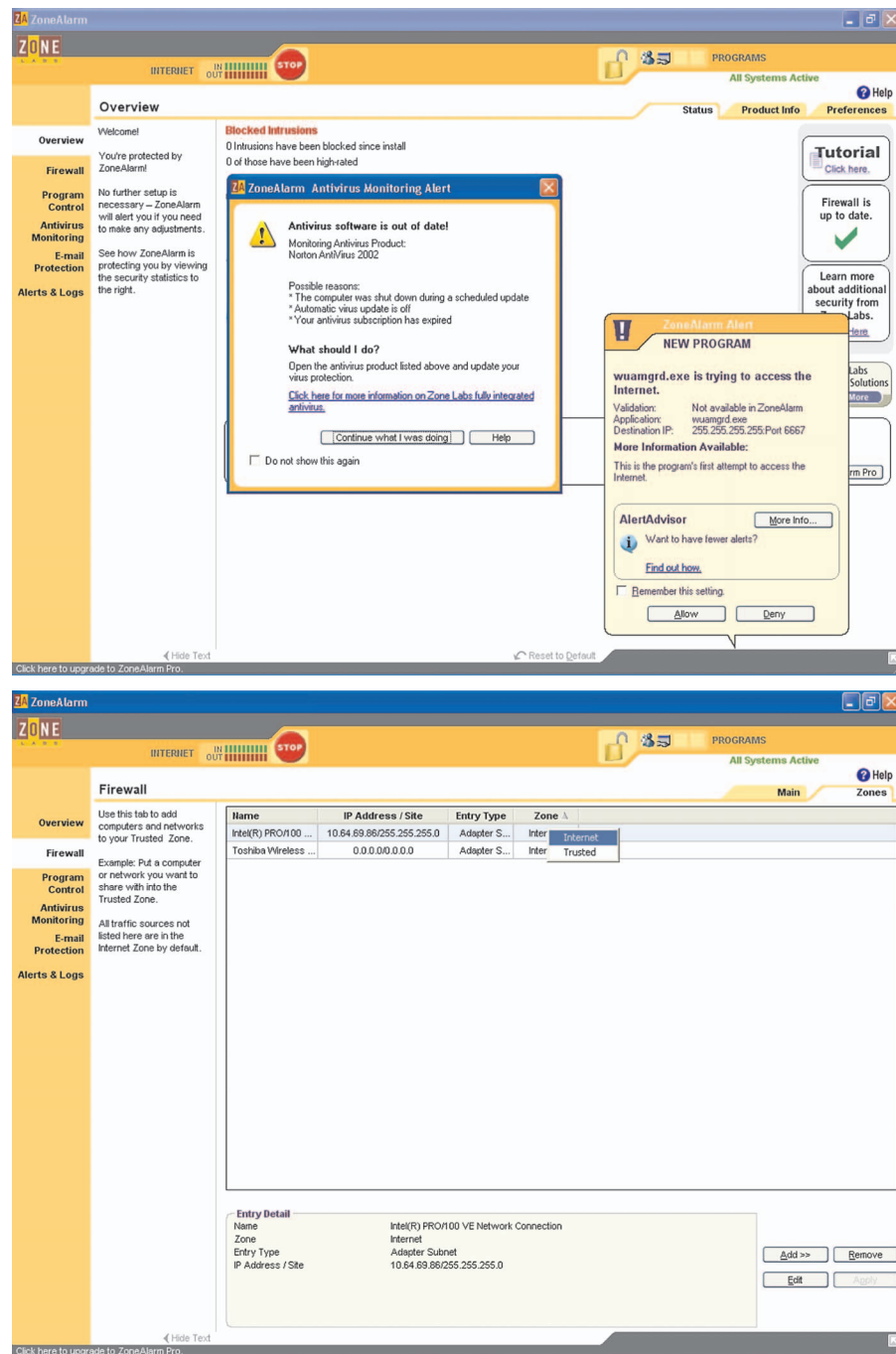
Dan satu lagi yang terakhir adalah fasilitas *E-mail Protection* yang akan memeriksa dulu setiap e-mail yang masuk, apakah terjangkit virus atau tidak. E-mail dengan *attachment .VBS* dijamin tidak

akan bisa lewat jika Anda memasang fitur ini dalam jaringan. Sayangnya, versi gratis ini hanya menyaring attachment *.VBS* saja, semua fitur lengkapnya dapat Anda gunakan pada versi komersialnya. Meski demikian, e-mail Anda sudah jauh lebih aman dari virus.

Manajemen yang Baik Perlu

Mengatur jaringan komputer agar bekerja lebih efisien tidaklah terlalu

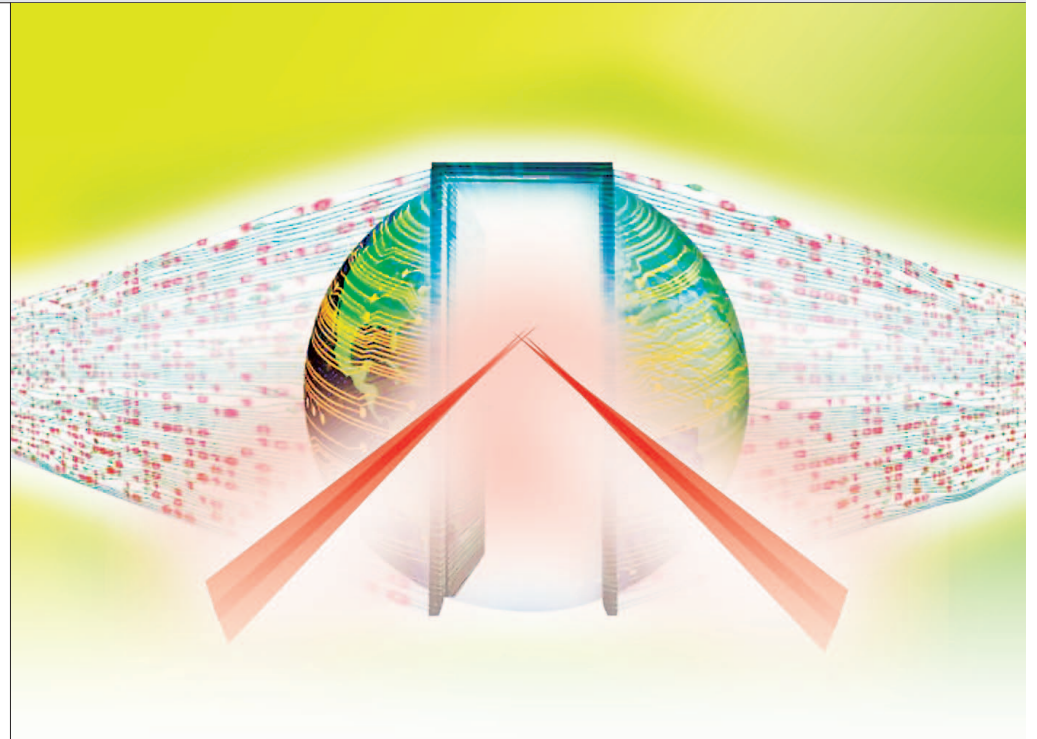
sulit. Kunci utamanya sebenarnya adalah melakukan monitoring dengan baik. Ketika jaringan Anda sudah termonitor dengan benar, semua pengaturan lainnya dapat juga berjalan dengan baik. Melakukan pengaturan bandwidth dan menentukan peraturan firewall menjadi lebih mudah. Aturlah dan pantaulah jaringan Anda mulai dari sekarang untuk mendapatkan kinerja jaringan yang lebih optimal. Selamat mencoba! ■



Mulai dari pemblokiran *traffic* mencurigakan sampai kinerja antivirus dan e-mail bersih juga diurus oleh *Zone Alarm*.

Metode pengamanan ala brankas ternyata juga dapat dilakukan di dalam sistem pengamanan jaringan komputer. Sistem ini diberi nama cukup unik, yaitu *Port knocking*.

Hayri



Port Knocking: Metode Pengamanan ala Brankas

► Jika berbicara soal keamanan jaringan komputer, mungkin komponen yang akan sering dibicarakan adalah seputar *firewall* beserta celah-celah keamanan jaringan itu sendiri. Celah-celah keamanan dapat terbuka biasanya dikarenakan perangkat komputer milik Anda tersebut diinstalasi dengan “sesuatu”. Anda mungkin menginstalnya dengan aplikasi pengolah dokumen, aplikasi *e-mail client*, aplikasi antivirus, aplikasi server client, dan banyak aplikasi yang mungkin Anda butuhkan bahkan mungkin juga tidak. Bisa saja Anda menginstalnya dengan sengaja maupun tanpa disengaja.

Aplikasi-aplikasi yang Anda instal, terutama yang dapat terhubung dengan jaringan dan Internet, biasanya akan membuka port-port komunikasi. Port-port komunikasi ini biasanya merupakan port-port yang ada dalam protokol TCP atau UDP yang merupakan anggota dari *Transportation layer* pada standar OSI. Melalui port komunikasi ini, dunia luar

dapat menjangkau perangkat Anda. Begitu pula sebaliknya, Anda juga bisa menjangkau mereka yang membuka port komunikasi tertentu. Komunikasi dapat berjalan dengan lancar, pertukaran informasi menjadi mudah dan kenyamanan Anda berkomputer bertambah dengan terbukanya port-port komunikasi ini.

Namun, kadang kala kenyamanan ini sering disalahgunakan oleh sebagian orang. Port-port komunikasi ini sering dijadikan sebagai celah untuk dimasuki secara ilegal. Port-port yang terbuka digunakan sebagai jalan menuju ke dalam jaringan internal atau ke server-server di dalamnya, kemudian mengcaukannya. Keterbukaannya yang bebas ini juga bisa menjadi salah satu ancaman bagi keamanan data Anda. Sangat mungkin penyusup masuk ke dalam komputer Anda, komputer di sebelah Anda, bahkan ke seluruh komputer di jaringan Anda jika dibiarkan terbuka sebebas-bebasnya.

Jika jumlah komputer yang terkoneksi ke jaringan sedikit, mungkin tidak akan sulit untuk mengetahui apa saja yang terinstal di masing-masing komputer. Namun, bagaimana jika jumlahnya sudah mencapai puluhan bahkan ratusan? Administrator jaringan mungkin tidak akan punya waktu untuk terus-menerus memantau apa yang telah terinstal di komputer-komputer tersebut. Untuk itulah, sebuah *firewall* sangat dibutuhkan untuk hadir di dalam jaringan Anda.

Firewall biasanya memiliki tugas utama melakukan pemblokiran terhadap port-port komunikasi yang terbuka di dalam sebuah jaringan. Di dalam firewall semua komunikasi keluar dan masuk dikontrol. Port-port yang tidak penting dapat diblokir di sini. Port-port yang penting dan berbahaya juga dapat diblokir di sini, sehingga hanya pihak yang Anda izinkan saja yang boleh masuk. Metode ini merupakan sistem pengamanan yang paling efektif dan banyak digunakan.

Namun terkadang, pemblokiran yang Anda lakukan sering menjadi senjata makan tuan. Ketika Anda butuh untuk menjalin komunikasi dengan apa yang ada di dalam jaringan Anda, firewall tidak mengizinkannya karena mungkin memang Anda berada pada area yang tidak diizinkan. Padahal komunikasi yang ingin Anda lakukan sangatlah penting untuk kelancaran kerja Anda.

Misalnya, Anda terkoneksi dengan Internet dan butuh masuk ke dalam web server Anda melalui SSH untuk memperbaiki konfigurasinya, sementara port SSH pada server tersebut dilarang untuk diakses dari Internet oleh firewall Anda. Tentu ini akan cukup merepotkan.

Untuk mengakali kejadian-kejadian seperti ini, ada sebuah metode yang cukup unik yang dapat dengan efektif menghilangkan masalah senjata makan tuan seperti ini. Metode tersebut diberi nama *Port Knocking*.

Apa Itu Port Knocking?

Secara harafiah, arti dari *Port Knocking* adalah melakukan pengetukan terhadap port-port komunikasi yang ada dalam sistem komunikasi data. Fungsi dan cara kerja dari sistem ini tidak jauh berbeda dengan arti harafiahnya.

Port knocking merupakan sebuah metode untuk membangun komunikasi dari mana saja, dengan perangkat komputer yang tidak membuka port komunikasi apapun secara bebas. Dengan kata lain, perangkat komputer ini tidak memiliki port komunikasi yang terbuka bebas untuk dimasuki, tetapi perangkat ini masih tetap dapat diakses dari luar. Ini dapat terjadi jika Anda menggunakan metode *Port Knocking*.

Koneksi dapat terjadi dengan menggunakan metode pengetukan port-port komunikasi yang ada. Pengetukan port-port ini dilakukan dengan kombinasi tertentu secara berurutan dalam satu rentan waktu tertentu.

Jika kombinasi dari pengetukan tersebut sesuai dengan yang telah ditentukan, maka sebuah port komunikasi yang diinginkan akan terbuka untuk Anda. Setelah terbuka, Anda bebas mengakses apa yang ada dalam jaringan tersebut melalui port komunikasi yang baru terbuka tadi. Setelah selesai melakukan

pekerjaan dan kepentingan Anda, port komunikasi yang tadi terbuka dapat ditutup kembali dengan melakukan pengetukan sekuensialnya sekali lagi. Maka, perangkat komputer dan jaringan Anda akan kembali aman.

Apa Gunanya Port knocking?

Jika dilihat sesaat, *Port Knocking* memang tidak terlalu banyak gunanya dan tidak terlalu istimewa. Hanya melakukan buka tutup port komunikasi saja tentu tidaklah terlalu banyak gunanya bagi pengguna jaringan lokal. Namun bagi para pekerja telekomuter, para pengguna komputer yang sering bekerja di luar kantor atau para administrator jaringan dan server yang harus mengurus server-server mereka 24 jam dari mana saja, Port Knocking merupakan metode yang luar biasa sebagai sebuah jalan penghubung ke perangkat-perangkat komputer mereka.

Port knocking cocok untuk mereka yang masih ingin memperkuat sistem keamanan komputer dan perangkat jaringannya, sementara tetap pula ingin memiliki koneksi pribadi ke dalamnya secara kontinyu dan dapat dilakukan dari mana saja.

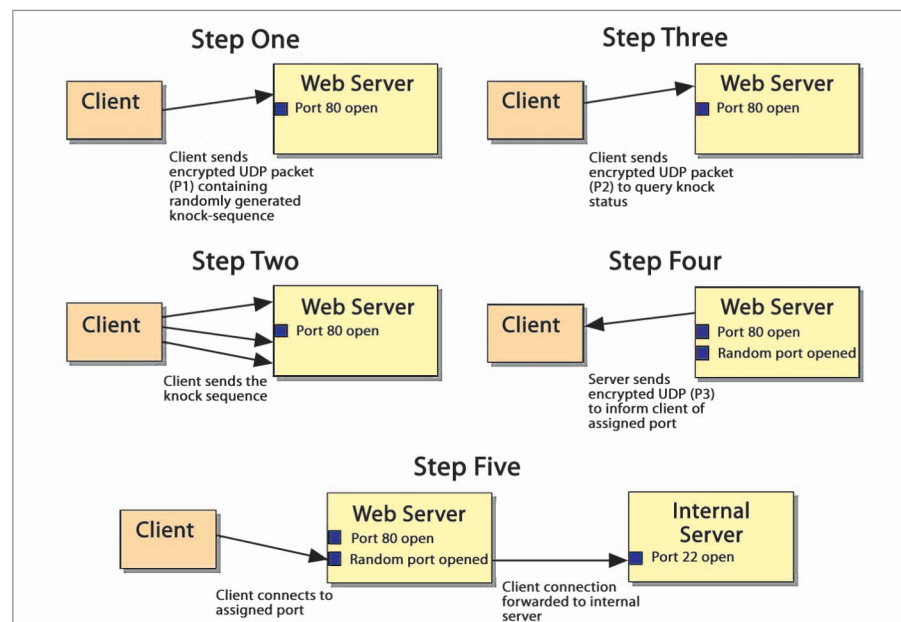
Komunikasi pribadi maksudnya koneksi yang tidak terbuka untuk umum seperti SMTP atau HTTP. Biasanya komunikasi pribadi ini lebih bersifat administratif dan

menggunakan servis-servis seperti telnet, SSH, FTP, TFTP, dan banyak lagi. Komunikasi pribadi ini akan sangat berbahaya jika dapat juga dilakukan oleh orang lain yang tidak berhak. Dengan menggunakan Port knocking, servis-servis tersebut akan tetap tertutup untuk diakses oleh publik, namun masih dapat secara fleksibel di buka oleh siapa saja yang memiliki kombinasi ketukan port-nya.

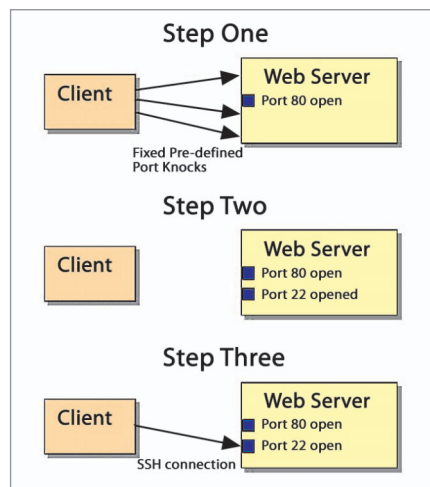
Bagaimana Cara Kerja Port Knocking?

Port knocking bekerja seperti halnya brankas dengan kunci kombinasi angka putar. Pada brankas tersebut, Anda diharuskan memutar kunci kombinasi beberapa kali hingga tepat seperti yang ditentukan. Sebenarnya Anda memutar lapisan-lapisan kunci di dalam brankas. Dalam lapisan-lapisan kunci tersebut terdapat sebuah lubang kunci. Jika sebuah putaran tepat, maka sebuah lubang terbuka. Jika seluruh putaran dilakukan dengan kombinasi yang benar, maka seluruh lubang terbuka dan menciptakan sebuah jalur khusus yang bebas tidak ada hambatan sama sekali. Jalur lubang kunci tadi tidak lagi menjadi penghalang pintu brankas untuk dibuka, sehingga pintu dapat terbuka dengan mudah.

Port knocking juga menggunakan sistem yang hampir sama, yaitu menggunakan kombinasi lapisan-lapisan kunci



Teknik yang lebih rumit dapat digunakan pada sistem *Port knocking* ini, seperti melakukan *port redirect* lagi untuk menuju ke port yang di inginkan. Tentu sistem ini akan lebih aman.



Cara kerja Port knocking sederhana.

untuk dapat mengamankan sebuah port komunikasi. Perbedaannya ada pada lapisan kunci yang digunakannya. Kunci dari sistem port knocking adalah port-port komunikasi itu sendiri. Cara membuka kuncinya adalah dengan mengakses dengan sengaja beberapa port komunikasi yang memang tertutup.

Ketika beberapa port komunikasi tadi diakses dengan kombinasi tertentu, maka akan terbuka sebuah port komunikasi baru yang bebas Anda masuki. Sebagai contoh, untuk membuka port 22 yang merupakan port komunikasi untuk aplikasi *remote login* SSH, Anda diharuskan “mengetuk” port 450, 360, 270, 180. Ketika kombinasinya benar dalam suatu waktu tertentu, maka akan terbuka port 22 yang Anda inginkan.

Sistem seperti ini dapat tercipta dengan bantuan sebuah program firewall. Program firewall biasanya memiliki fasilitas untuk melakukan *logging* terhadap setiap proses komunikasi yang keluar-masuk melaluinya. Dari membaca log inilah, sistem Port knocking dapat mengetahui kombinasi ketukan. Ketika sistem Port knocking membaca sebuah kombinasi yang tepat pada log, maka sebuah proses otomatis menjalankan aplikasi yang akan membuka port komunikasi yang ditentukan. Setelah terbuka, maka jadilah sebuah pintu masuk kedalam perangkat Anda.

Apa Bedanya dengan VPN?

Jika hanya ingin membangun koneksi secara pribadi dari mana saja, mengapa tidak menggunakan VPN saja? Mungkin

ada juga pertanyaan seperti itu diajukan terhadap teknologi *Port Knocking*. VPN memang teknologi yang selama ini digunakan untuk membangun koneksi yang bersifat *private* dari mana saja di seluruh dunia.

Salah satu media yang digunakannya adalah Internet. Melalui VPN, Anda dapat terkoneksi dengan server-server Anda di kantor pusat meskipun Anda tengah berada di luar kota maupun luar negeri, asalkan ada koneksi Internet.

VPN bekerja dengan membangun sebuah terowongan atau sering disebut dengan istilah *tunnel*. Sebuah tunnel atau terowongan memiliki fungsi untuk membuat sebuah jalur khusus bagi objek yang ingin dilewatkannya. Jalur khusus tersebut tidak akan terganggu oleh apapun di luarnya. Bahkan Anda tidak dapat melihat apa yang sedang lalu-lalang di dalam terowongan tersebut. Seakan-akan apa yang mengalir di dalamnya memiliki jalur langsung atau *point-to-point* dari lokasi pengiriman ke tujuannya.

Begitu pula VPN, seakan-akan Anda memiliki sebuah koneksi point-to-point ke lokasi yang ingin Anda tuju, padahal untuk terhubung ke sana data tersebut akan melalui jalur Internet.

Untuk membuat VPN, biasanya dibutuhkan sebuah server atau *hardware* spesifik yang memiliki kemampuan itu. Jika server yang digunakan, mungkin server tersebut harus diinstalasi dengan berbagai macam aplikasi, dengan berbagai pengaturan khusus dan spesifikasi tertentu, dan memakan waktu cukup lama untuk menyiapkannya. Jika menggunakan *hardware* khusus tentu akan lebih mudah, tetapi Anda harus mengeluarkan biaya tambahan untuk itu.

Membuat sistem Port Knocking jauh lebih mudah daripada membuat VPN. Fungsi dan keunggulannya banyak memiliki persamaan, meskipun cara kerja dan metode yang digunakannya sangat jauh berbeda.

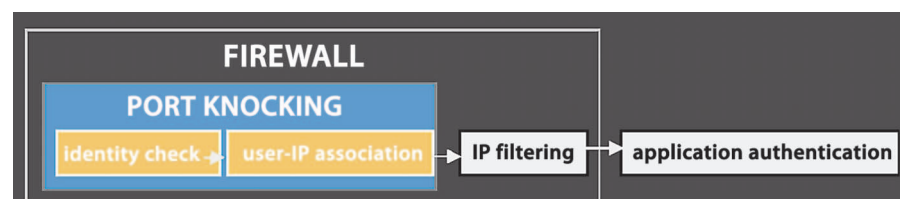
Untuk menghubungkan Anda ke jaringan lokal, Port knocking dapat digunakan untuk membuka servis-servis tertentu yang dapat digunakan untuk melakukan *remote login*. Misalnya dengan menggunakan servis SSH untuk dapat masuk ke dalam sebuah server yang juga terkoneksi ke dalam jaringan lokal.

Tetap Aman dan Juga “Sedikit” Nyaman

Mau jaringan komputer Anda aman dan juga nyaman? Mungkin sangat sulit untuk membuat jaringan yang benar-benar aman namun juga sangat nyaman. Baik sang administrator maupun pengguna pasti akan merasakan betapa tidak nyamannya untuk berada dalam sebuah jaringan yang keamanannya hebat. Sang admin harus selalu bekerja rajin untuk mengawasi dan menutupi celah-celah yang hampir tidak ada putus-putusnya. Para pengguna pun akan merasa tidak bebas bergerak jika koneksi ke sana-ke mari selalu dibatasi dan diawasi.

Namun dengan adanya *Port knocking*, rasanya mereka akan mendapatkan sedikit angin segar. Di mana keamanan dibuat menjadi lebih fleksibel daripada yang sudah-sudah. Sang administrator tidak akan kerepotan mengawasi port-port komunikasi yang terbuka bebas. Para pengguna pun dapat membuka sendiri port komunikasi yang diinginkan dengan berbagai macam kombinasi ketukan.

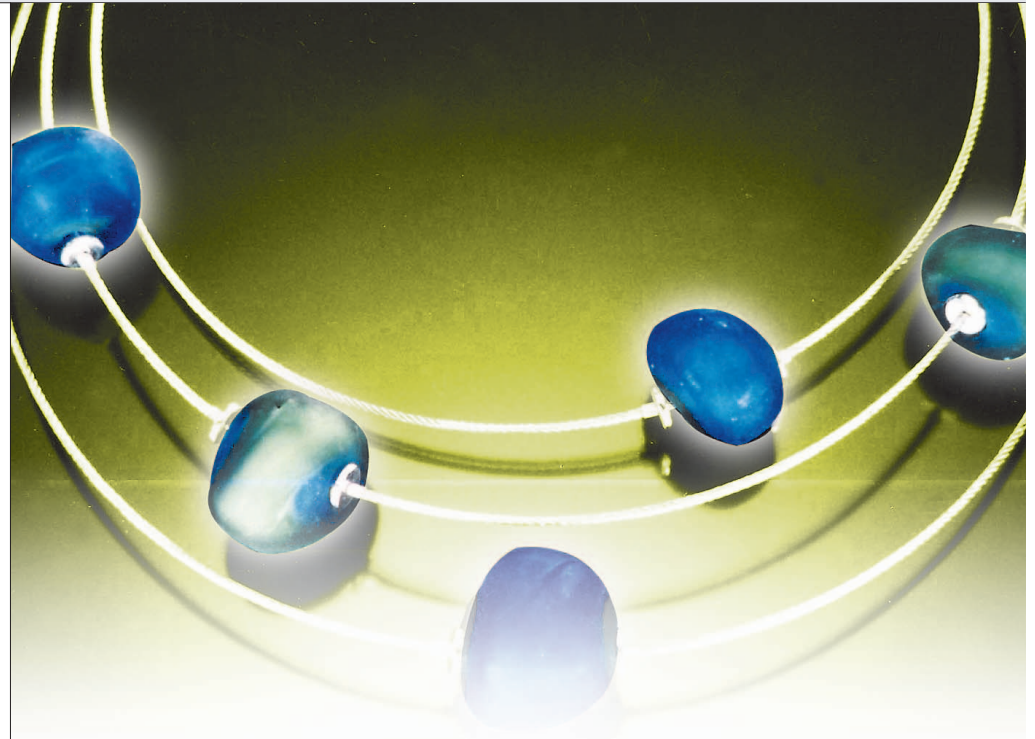
Tetapi, Anda juga tidak boleh lengah begitu saja. Mungkin saja beberapa bulan lagi, berapa minggu atau bahkan berapa hari lagi, metode Port knocking tidak lagi begitu aman karena kerja iseng para *hacker* yang dapat menjebolnya. Kemungkinan itu bisa saja terjadi kapan saja, namun paling tidak Port knocking sudah membuat mereka lebih susah dan kenyamanan Anda juga akan sedikit bertambah. Selamat mencoba! ■



Firewall sangat berperan besar dalam membuat sistem Port knocking ini.

Beberapa tahun ke depan, fungsi perhiasan akan mengalami sedikit perubahan. Bukan lagi sebagai pelengkap penampilan seseorang, namun juga berfungsi sebagai alat Bantu yang canggih. Mulai dari anting yang juga berfungsi sebagai anting dan kalung sebagai mikrofon, sampai gelang yang berfungsi sebagai ponsel.

Fadilla Mutiarawati



Perhiasan Digital Masa Depan

► Di masa yang akan datang, teknologi digital tidak hanya akan berada dalam perangkat komputer dan rumah tangga saja, melainkan juga pada perhiasan yang akan Anda gunakan nanti. Gabungan antara kecanggihan teknologi digital dengan teknologi nano dapat memungkinkan sebuah benda dengan tingkat kecanggihan yang tinggi memiliki bentuk fisik yang sangat kecil. Sangat kecilnya sampai tidak sulit untuk meletakkannya ke dalam perhiasan seperti cincin atau kalung.

Jika dulu menonton film seperti "Star Trek" dianggap hanya berisi dengan khayalan saja, maka sebentar lagi hampir semua yang dilihat di dalamnya akan menjadi nyata. Seperti berbicara dengan menggunakan bros kecil saja. Masuk ke dalam ruangan hologram, kini semuanya terlihat sangat mungkin.

Dulu telewicara dengan menggunakan telepon dianggap tidak mungkin, sekarang *video conference* dapat dilakukan melalui Internet dengan perangkat yang sangat murah. Bahkan sebentar lagi hal ini juga dapat Anda lakukan melalui gelang di pergelangan Anda. Oleh sebab itu, apa yang diimpikan pada masa lalu

tentang masa depan semakin hari terlihat semakin mungkin.

Salah satu perusahaan TI yang sangat berperan besar untuk mewujudkan perhiasan berteknologi canggih ini adalah IBM. Selain IBM, masih ada juga beberapa badan penelitian lain yang ikut mengembangkannya. Dan salah satu teknologi yang ikut berperan besar dalam pembuatan perhiasan canggih ini adalah teknologi *wireless Bluetooth*.

Berikut ini adalah perhiasan-perhiasan yang tengah dikembangkan sekarang:

Anting

Apa yang dapat diselipkan ke dalam anting? Salah satu yang paling mungkin adalah *wireless speaker*. Letak anting yang sangat dekat dengan telinga, membuat speaker sangat cocok untuk diletakkan di dalamnya.

Sebenarnya, *wireless speaker* sudah dapat Anda miliki saat ini. Namun tentu saja terhubung bentuknya yang tidak semewah anting, maka *wireless speaker* tersebut tidak disebut sebagai perhiasan melainkan hanya *earphone* saja.

Speaker ini dinamakan *Bluetooth headset*. Kata *Bluetooth* digunakan

karena memang speaker tanpa kabel tersebut menggunakan teknologi *wireless Bluetooth*. Sedangkan penggunaan kata *headset* sendiri karena pada alat ini, selain terdapat speaker juga terdapat mikrofon yang berintegrasi langsung dengan speaker-nya.

Bluetooth headset yang ada saat ini sudah banyak dikembangkan oleh berbagai produsen perangkat telekomunikasi maupun TI di seluruh dunia. Seperti Nokia, Ericsson, Siemens, dan



Tidak hanya wanita saja yang dapat berkomunikasi dengan aksesoris di pergelangan tangannya.



Gelang masa depan yang dikembangkan oleh IBM.

masih banyak lagi. Bahkan Bluetooth headset tidak hanya dapat digunakan untuk keperluan telekomunikasi saja, melainkan juga untuk mendengarkan musik. Baik dengan menggunakan komputer atau menggunakan perangkat audio yang besar.

Saat ini, memang bentuk wireless speaker yang menggunakan teknologi Bluetooth masih memiliki bentuk yang cukup besar, sehingga kurang membuat pemilikinya terlihat cantik. Namun dengan pengembangan yang terus berlangsung dan hadirnya teknologi nano, maka tidak mustahil speaker Bluetooth ini mengecil. Sedemikian kecilnya hingga muat diletakkan ke dalam sebuah anting.

Kalung

Tidak hanya anting saja yang akan berubah fungsi, kalung juga dapat mengalami perubahan yang menarik. Bisa sebagai mikrofon, bisa juga sebagai kamera.

Letak kalung yang berdekatan dengan mulut sebagai sumber suara, membuat kalung sangat cocok digunakan sebagai mikrofon ponsel. Tentu saja hal ini akan sangat membantu Anda, khususnya para wanita yang masih ingin berhubungan dengan sanak famili maupun rekan tanpa harus merusak penampilan.

Saat ini, sebuah mikrofon sudah dapat berbentuk sangat kecil, sama halnya dengan speaker. Sayangnya, mikrofon-mikrofon tersebut masih menggunakan kabel. Sedangkan jika tidak menggunakan kabel, maka bentuknya masih cukup besar. Namun bukan berarti, hal ini tidak akan dapat berubah mengingat sampai saat ini perkembangan teknologi masih berlangsung.



Headset canggih nan elegan yang dikembangkan oleh Charmed Technology.

Saat ini, sebuah perusahaan yang sedang mengembangkan teknologi dengan mengambil bentuk kalung adalah Nokia. Nokia mencoba untuk memproduksi sebuah kamera ponsel yang diletakkan pada kalung. Bentuknya sangat futuristik dan unik. Sehingga seseorang yang melihatnya tidak akan menyadari bahwa kalung tersebut memiliki fungsi ganda.

Gelang/Jam Tangan

Menggunakan gelang atau jam tangan sebagai alat komunikasi sudah sangat lama diimpikan manusia. Dan sekarang, hal tersebut lagi impian melainkan kenyataan. Sebab Samsung, salah satu produsen perangkat telekomunikasi sudah pernah memproduksinya.

Mungkin bentuknya memang belum sempurna masih dianggap terlalu besar dan kokoh, sehingga bagi wanita ponsel ini dianggap kurang cantik. Oleh sebab itu, teknologi ini masih terus dikembangkan, baik oleh IBM maupun oleh beberapa produsen perangkat TI lainnya. Sehingga di masa yang akan datang, seseorang tidak perlu lagi menenteng ponsel atau komputer ke mana-mana. Mereka cukup menggunakan perhiasannya dan tetap terhubung.

Cincin

Cincin adalah salah satu yang sangat umum digunakan oleh seseorang baik perempuan ataupun laki-laki. Apa yang dapat disimpan dalam sebuah cincin, ternyata sangat beragam.

Salah satu cincin digital yang sudah dikembangkan oleh Dallas Semiconductor adalah Java Ring. Dengan Java Ring, semua *password* yang berhubungan baik dengan komputer maupun pintu ke



Medallion, kalung berfungsi sebagai kamera dari Nokia.

ruangan tertentu dapat disimpan. Dan secara otomatis cincin ini akan membuka *password* pada setiap saat *password* tersebut dibutuhkan. Untuk dapat bekerja, cincin ini membutuhkan sebuah reader yang dipasangkan pada alat (baik pintu maupun komputer) yang membutuhkan *password* yang berada di dalam cincin tersebut. Reader ini dinamakan Blue Dot Receptor.

Tidak Hanya Wanita

Apa yang disebut dengan *digital jewelry* atau perhiasan digital ini tidak hanya milik kaum perempuan saja. Seorang lelaki juga dapat memanfaatkan teknologi tersebut sama halnya dengan kaum perempuan.

Bukankah saat ini sudah banyak laki-laki yang menggunakan anting dan kalung. Apalagi cincin dan jam tangan. Oleh sebab itu, jangan menganggap bahwa teknologi ini tidak akan bermanfaat untuk kaum lelaki.

Bahkan ada kecenderungan membuat perhiasan digital untuk laki-laki lebih mudah daripada untuk perempuan, sebab kaum lelaki lebih cenderung menggunakan perhiasan yang lebih besar ketimbang perempuan, seperti cincin dan jam tangan. Bukankah begitu?

Setelah buku dan perhiasan, apa lagi yang akan menjadi digital? Mungkin saja baju, celana, dan semua pakaian yang Anda pakai di masa yang akan datang juga dapat menjadi sebuah komputer berjalan. Siapa tahu? ■



Cincin berteknologi Java.

Pernah memikirkan apa arti nama di atas? Artikel ini merupakan panduan Anda untuk file DirectX.

Gunung Sarjono



Seputar DirectX

► *Game* dan aplikasi multimedia adalah beberapa dari program paling memuaskan yang bisa didapatkan untuk PC Anda, tetapi menjalankan mereka dengan baik tidak selalu semudah yang diharapkan. Pertama, arsitektur PC tidak pernah didesain untuk *gaming platform*. Kedua, luasnya *range* PC menyebabkan komputer yang satu dapat berbeda dengan yang lain. Jika *game console* semua berisi *hardware* yang sama, maka PC tidak: besarnya *range* perbedaan dapat membuat sakit kepala pada waktu hendak bermain game.

Untuk mengurangi rasa sakit tersebut, Microsoft perlu memperkenalkan standar umum yang dapat diikuti oleh semua game dan aplikasi multimedia—*interface* antara *operating system* dan hardware apapun yang terinstal dalam PC. Interface umum ini adalah DirectX, sesuatu yang dapat menjadi sumber banyak kebingungan.

DirectX merupakan suatu interface yang didesain untuk mempermudah *programming*, baik bagi pengembang game dan kita yang hanya ingin duduk santai dan memutar *blockbuster* terbaru. Namun sebelum kita melihat apa

itu DirectX dan bagaimana ia bekerja, kita perlu sedikit melihat sejarahnya.

Sejarah DirectX

Setiap *game* perlu melakukan tugas tertentu secara berulang-ulang. Ia perlu melihat input dari mouse, joystick, atau keyboard, dan ia perlu menampilkan gambar layar dan memutar suara atau musik. Itulah yang dilakukan setiap game pada tingkat yang paling sederhana.

Bayangkan seberapa kompleks ini bagi programmer pada awal arsitektur PC sebelum Windows. Setiap programmer perlu membuat cara mereka sendiri dalam membaca keyboard atau mendeteksi apakah joystick terhubung, dan hanya digunakan untuk bermain game. Bahkan diperlukan rutin khusus untuk menampilkan gambar paling sederhana pada layar atau memutar suara sederhana.

Pada dasarnya, programmer game berbicara secara langsung ke *hardware* PC pada tingkat dasar. Pada waktu Microsoft memperkenalkan Windows, itu merupakan sangat penting bagi stabilitas dan kesuksesan PC di mana sesuatunya dipermudah baik bagi pengembang dan pemain. Lagipula,

siapa yang mau menulis game untuk suatu mesin jika mereka harus menemukan kembali rodanya setiap kali mereka membuat game baru? Ide Microsoft adalah sederhana: hentikan programmer berbicara secara langsung kepada hardware, dan sebagai gantinya buat *toolkit* umum yang dapat mereka gunakan. Dari sini lahirlah DirectX.

Teknologi ini kali pertama diperkenalkan pada tahun 1995 dan menjadi standar untuk pengembangan aplikasi multimedia pada *platform* Windows.

Bagaimana DirectX Bekerja?

Secara mendasar, DirectX merupakan *interface* antara *hardware* dalam PC Anda dan Windows itu sendiri, yang merupakan bagian dari Windows API (*Application Programming Interface*).

Mari lihat contoh praktis. Pada waktu pembuat game ingin memutar file suara, ini hanyalah masalah menggunakan fungsi *library* yang sesuai. Pada waktu game berjalan, ia memanggil DirectX API, yang akan memutar file suara. Pembuat game tidak perlu tahu jenis sound card apa yang dihadapi, apa yang dapat dilakukannya, atau bagaimana berbicara

kepadanya. Microsoft telah menyediakan DirectX, dan pabrikan sound card telah menyediakan driver yang berkemampuan DirectX. Ia menanyakan suara yang ingin dimainkan, hanya itu—pada mesin apapun ia dijalankan.

Dari sisi kita sebagai *gamer*, DirectX juga memberikan kemudahan yang besar—paling tidak secara teori. Anda menginstal sound card baru di tempat yang lama, yang datang dengan driver DirectX. Lain waktu memainkan game Anda masih dapat mendengar suara dan musik, dan Anda tidak perlu melakukan perubahan konfigurasi yang kompleks.

Pada awalnya, DirectX hanyalah toolkit sederhana: hardware masa awal terbatas dan pada waktu itu hanya dibutuhkan fungsi grafis yang sederhana. Seiring dengan perkembangan hardware dan *software* yang semakin kompleks, demikian juga DirectX. Ia sekarang lebih dari sekadar toolkit grafis, dan ia telah meliputi banyak rutin yang menangani semua jenis komunikasi hardware.

Sebagai contoh, rutin DirectInput dapat menangani semua jenis perangkat input, dari mouse sederhana dengan dua-tombol sampai *flight joystick* yang kompleks. Bagian lain adalah DirectSound untuk perangkat audio dan DirectPlay yang menyediakan toolkit untuk bermain game secara *online* atau *multiplayer*.

Versi DirectX

Versi DirectX terakhir pada saat artikel ini ditulis adalah DirectX 9.0c. Ia berjalan pada semua versi Windows dari Windows 98 sampai Windows Server 2003. Namun, ia tidak dapat dijalankan pada Windows 95: jika Anda mempunyai komputer yang menjalankan Windows 95, Anda sudah mentok pada versi 8.0a. Windows NT 4 juga membutuhkan versi tertentu—yaitu DirectX 3.0a.

Dengan banyaknya versi DirectX yang tersedia beberapa tahun belakangan, adalah sulit untuk mengetahui versi mana yang Anda butuhkan. Secara keseluruhan, semua versi DirectX *backwardly compatible*—game yang membutuhkan DirectX 7 akan dapat berjalan pada versi yang lebih baru,

tetapi tidak dengan yang lebih lama.

Banyak *game* yang secara eksplisit menyatakan bahwa mereka membutuhkan DirectX 9, dan tidak dapat berjalan jika versi terbaru belum diinstal. Ini karena mereka menggunakan fitur baru yang terdapat pada versi tersebut, walaupun *developer* malas sering menggunakan versi paling terakhir untuk game yang bersangkutan, padahal tidak menggunakan satupun peningkatan baru yang ada. Namun pada umumnya, jika suatu game terikat versi tersebut, Anda perlu *upgrade* sebelum bermain. Peningkatan pada kode DirectX berarti peningkatan pada banyak game pada waktu Anda meng-upgrade ke DirectX terakhir.

Apakah Saya Memerlukan DirectX 9.0?

Biasanya, setiap *game* yang menggunakan DirectX akan menginstal versi DirectX yang dibutuhkan agar game tersebut dapat berjalan. Oleh karena itu, pada umumnya Anda tidak perlu *download* DirectX 9.0 agar game Anda dapat berjalan. Namun, tidak ada salahnya menginstal DirectX 9.0.

Beberapa fitur baru yang terdapat pada DirectX 9.0 mungkin dapat mening-

katkan kualitas dan kinerja game tersebut. Di samping itu, banyak demo game yang tidak dilengkapi dengan DirectX, jadi Anda mungkin perlu menginstal DirectX 9.0 jika ingin memainkan demo yang terbaru.

Meng-upgrade DirectX

Semua versi Windows yang tersedia datang dengan DirectX sebagai komponen inti sistem yang tidak dapat dihilangkan. Namun, banyak *game* baru membutuhkan versi paling terakhir supaya dapat berjalan dengan baik atau supaya dapat dijalankan.

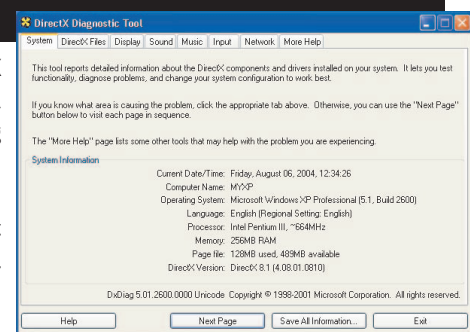
Biasanya, tempat terbaik untuk menginstal DirectX versi terbaru adalah dari situs Web Microsoft, yang dapat ditemukan di www.microsoft.com/windows/directx. Anda dapat *download installer* sederhana yang nantinya akan *download* komponen yang perlu diinstal oleh sistem, atau *download* langsung paket lengkap untuk instalasi secara *offline*. Salah satu sumber lain dari DirectX adalah game itu sendiri. Jika game membutuhkan suatu versi tertentu, itu akan ada di CD instalasi dan mungkin otomatis diinstal oleh installer game tersebut. ■

ANALISIS MASALAH DIRECTX

■ Menganalisis masalah instalasi DirectX dapat menyulitkan, terutama jika Anda tidak mengetahui bagian mana yang menyebabkan *game* tidak dapat dimainkan. Untungnya, Microsoft menyediakan utility bernama DirectX Diagnostic Tool. Anda tidak akan menemukan tool ini pada *Start Menu* pada Windows versi berapapun, dan masing-masing cenderung menginstal pada tempat yang berbeda.

Cara paling mudah untuk menggunakannya adalah dengan membuka dialog *Run* dari *Start Menu*, ketik dxdiag dan kemudian klik OK. Pada waktu pertama dijalankan, ia membutuhkan beberapa detik untuk menandai instalasi DirectX dan memeriksa jika ada masalah.

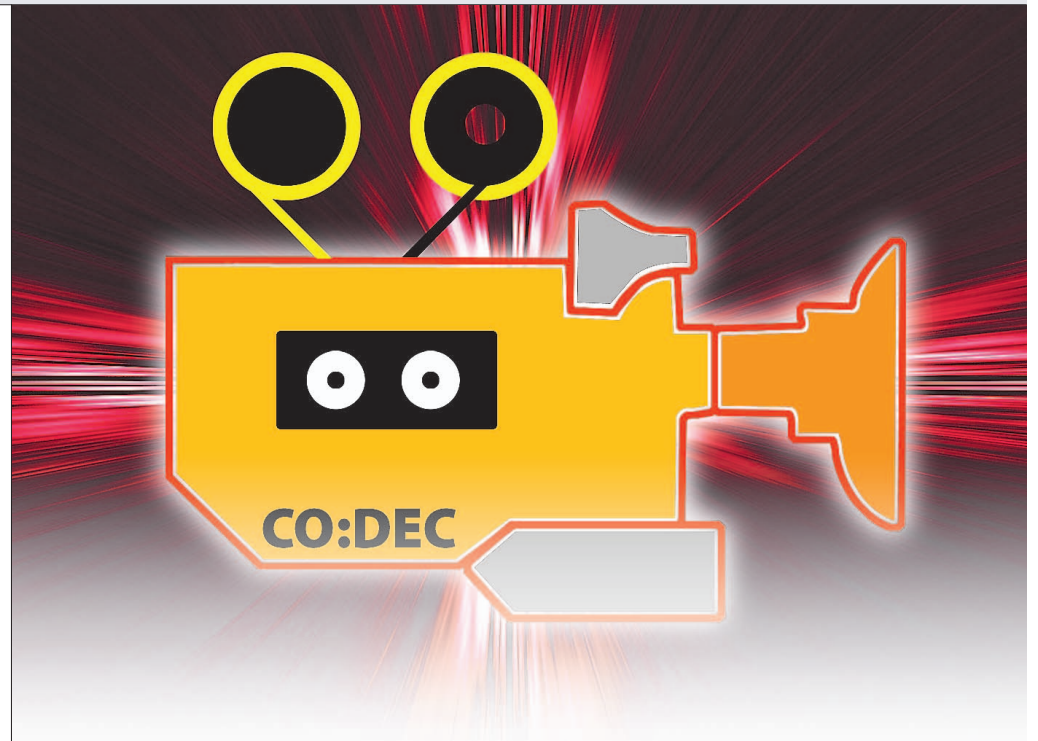
Tab DirectX File menampilkan versi setiap file yang digunakan. Notes pada bagian bawah perlu Anda lihat, karena file yang hilang atau terkorupsi akan ditandai di sini. Tab *Display*, *Sound*, *Music*, *Input*, dan *Network* semua berhubungan dengan bagian tertentu dari DirectX, dan semua kecuali tab *Input* menyediakan tool untuk mengetes fungsi *hardware*. Yang terakhir, tab *More Help* memberikan cara mudah untuk menjalankan DirectX *Troubleshooter*, cara Microsoft dalam memecahkan masalah umum DirectX.



DirectX Diagnostic Tool.

Mengapa PC Anda mau memutar beberapa file video dan beberapa tidak? Semuanya kembali ke codec.

Gunung Sarjono



Sekilas tentang Video Codec

► Video digital telah mengambil alih penyimpanan analog dengan cara yang besar. Dari film DVD ke *camcorder*, *player* saku, bahkan telepon selular dengan fasilitas perekaman video, semua perangkat media digital ini mempunyai satu persamaan umum dengan PC Anda: kurangnya tempat penyimpanan.

Video digital memakan tempat penyimpanan yang sangat besar, terutama pada resolusi yang lebih tinggi. Mungkin banyak klip yang Anda lihat pada situs web tidak membutuhkan tempat yang besar, tetapi video PAL dengan resolusi penuh 720x576 yang digunakan oleh DVD dan digital camcorder bisa memakan ratusan megabytes tiap menit. Karena tak seorang pun dari kita mempunyai kapasitas penyimpanan tanpa batas, file video perlu dikurangi ukurannya untuk membuat mereka praktis.

Apakah Codec?

Windows melakukan ini dengan menggunakan bagian dari *software* yang disebut *codec*. Kata *codec* berarti COmpressor/DECompressor: suatu rutin *software* yang mengompres video

mentah untuk disimpan, dan kemudian mengdekompresnya untuk ditampilkan pada PC Anda.

Sebelum melihat bagaimana video codec bekerja, kita perlu memperjelas suatu miskonsepsi. Anda mungkin mendengar bahwa AVI adalah sebuah format—ia bukan. Secara teknis, AVI merupakan sudah wadah atau pembungkus, sama seperti QuickTime-nya Apple.

Suatu wadah bisa dianggap penyalur, jika Anda suka. Dalam hal file AVI, ia merupakan cara untuk mentranspor aliran video dan audio di dalam file yang sama. Satu file AVI dapat berbeda satu dengan yang lain, meskipun mereka berisi video dan audio yang sama pada resolusi yang sama. Penyebabnya adalah sederhana: video yang disimpan di dalam file AVI dapat dikompres dengan codec berbeda, sesuatu yang tidak dapat Anda ungkapkan hanya dengan memutar file tersebut.

Audio codec dapat *lossy* atau *lossless*, tetapi video codec pada umumnya *lossy*. Video yang dikompres dengan *lossy* codec tidak sama dengan rekaman aslinya, karena ada informasi yang

diabaikan pada waktu kompresi untuk mengurangi ukuran file. Jumlah data yang terdapat pada file video resolusi tinggi sangat banyak sehingga tidaklah praktis untuk menggunakan kompresi *lossless*.

Frame dan Field

Secara luas, video codec dapat dibagi ke dalam dua jenis: *frame-based* dan *field-based* atau *temporal codec*. *Frame-based* codec seperti Cinepak, atau Motion-JPEG bekerja dengan melihat dan mengompres setiap frame video secara terpisah. Dengan 25 frame per detik dalam PAL video, *frame-based* codec mempunyai dua kerugian: mereka dapat menjadi lambat dan ukuran file dapat cukup besar.

Film, tentunya, merupakan urutan gambar diam yang dijalankan pada kecepatan konstan sehingga tercipta suatu ilusi gerakan. Dengan pikiran tersebut, tidaklah sulit untuk melihat bahwa setiap frame atau gambar akan tampak sama dengan sebelum dan sesudahnya, dengan sedikit perbedaan di mana objek telah berpindah. Mengapa mengompres setiap frame secara indi-

vidu, padahal sebagian besar dari mereka pada dasarnya sama?

Di sinilah field atau temporal codec mengambil peranan. Temporal codec melihat bagaimana aliran video berubah seiring waktu. Pada waktu temporal codec mengompres suatu aliran, ia menyimpan frame pertama. Frame selanjutnya dibandingkan dengan frame tersebut, dan perubahan apa pun di antara keduanya di pisahkan.

Selanjutnya, codec hanya mengompres perubahan antara frame pertama dan frame berikutnya. Karena frame pertama ini penting dan menyimpan informasi yang dibutuhkan untuk mendekompres frame berikutnya, ia dikenal sebagai *keyframe*. Pada waktu codec menemukan perbedaan yang besar seperti ketika film berpindah ke adegan yang berbeda, ia mengambil dan mengompres *keyframe* lain.

Seperti yang dapat Anda bayangkan, temporal codec paling efisien pada waktu menangani rekaman yang tidak berubah banyak. Temporal codec yang paling terkenal adalah MPEG. MPEG-2, revisi dari standar orisinal yang mempunyai resolusi tinggi, merupakan codec yang digunakan untuk mengemas seluruh film *blockbuster* pada disc DVD.

Windows Playback

Pada waktu Anda memutar file video yang disimpan dalam format misalnya sebagai file MPG, Windows secara otomatis mengetahuinya dan segera menangani file tersebut. Format seperti AVI jauh lebih kompleks, karena video dan audio *stream* dapat menggunakan banyak codec kompresi. Pertama, Windows memeriksa sebagian AVI header yang berisi kode FourCC—kode empat digit

yang digunakan untuk mengidentifikasi kode yang digunakan dalam *stream*.

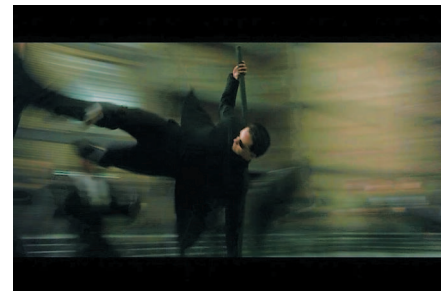
Windows kemudian membandingkan kode tersebut dengan video codec yang Anda punya pada PC dan memilih *playback codec* yang sesuai. Jika Anda tidak mempunyai codec yang dapat memutar kode FourCC tersebut, maka Anda akan berada dalam masalah—Windows akan menolak memutar file tersebut.

Setelah video dan audio codec ditentukan, Windows kemudian memberikan *stream* tersebut ke codec untuk didekompresi. Codec kemudian memberikan dekomposisi ke program player yang Anda gunakan, apakah Windows Media Player atau aplikasi pihak ketiga seperti WinAmp. Dengan model modular seperti ini, codec dapat digunakan untuk aplikasi manapun untuk memutar file video tanpa perlu programmer menuliskan rutin dekomposisi mereka setiap waktu.

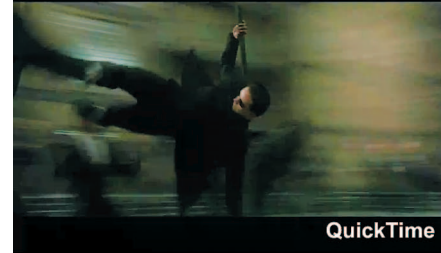
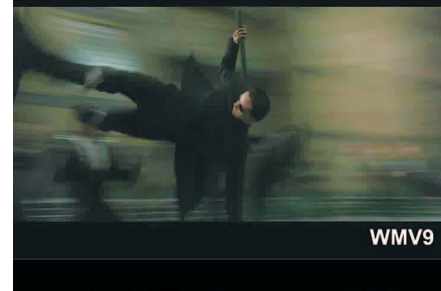
Mencari Codec

Dengan adanya puluhan video codec yang dapat digunakan, setiap file AVI yang Anda jumpai bisa menjadi suatu pertarungan. Apakah sistem Anda dilengkapi dengan codec yang sesuai untuk memutar video dan audio *stream* dengan benar? Jika tidak Anda akan segera mengetahuinya, pada waktu Windows mengeluh bahwa ia tidak mempunyai kode yang sesuai. Jika Anda membutuhkan suatu codec, di mana mencarinya?

Daripada menginstal semua codec, ada cara yang sederhana untuk mengetahui codec kompresi apa yang dibutuhkan oleh suatu file AVI—yaitu dengan menggunakan *software* bernama Gspot (www.headband.com/gspot/). Kali pertama Anda menjalankannya,



Adegan dari film "Matrix Reloaded" ini merupakan salah satu adegan yang sulit untuk dikompresi.



Hanya DivX di sini yang adegannya terlihat jelas.

Gspot mungkin terlihat sangat kompleks. Kenyataannya memang demikian, tetapi untuk mencari codec dapat dilakukan dengan mudah.

Jalankan Gspot, lalu buka file AVI. Setelah Gspot men-*scan* sistem, ia menampilkan sejumlah informasi tentang isi file tersebut. Yang Anda butuhkan terdapat pada bagian kanan di bawah *Video*. Bagian *Stat* memberitahukan apakah Anda mempunyai kode yang dibutuhkan. Jika tidak, pilih *View, Codec Database, Video*, dan cari kode *FourCC*. Gspot juga akan memberitahukan di mana Anda bisa mendapatkan codec yang hilang. ■

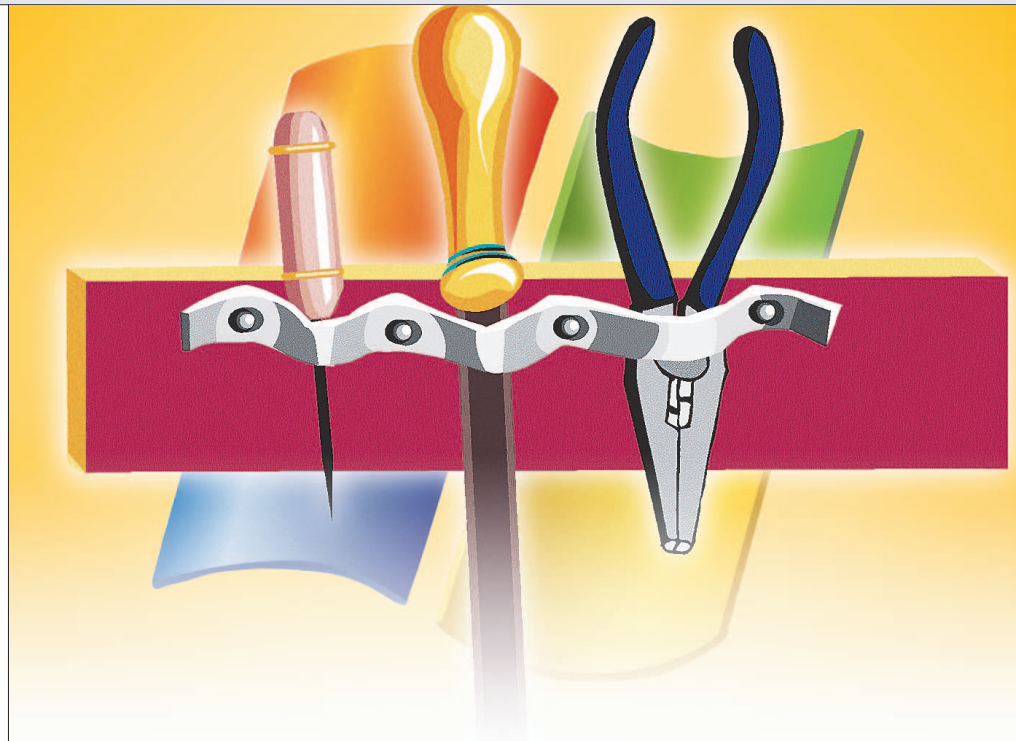
MPEG-4 YANG MENAKJUBKAN

■ Format dan codec video datang dan pergi seiring dengan waktu, beberapa sangat berguna sehingga mereka dapat maju dengan cepat. MPEG-4 merupakan suatu fenomena. Secara luas, ia merupakan standar untuk kompresi video yang sangat efisien ditambah lagi tampilannya yang indah yang melampaui apa yang dapat ditawarkan oleh format seperti standar DVD MPEG-2—paling tidak dalam hal kompresi.

Meskipun begitu, MPEG-4 lebih merupakan suatu standar daripada codec. Ada beberapa codec yang sesuai untuk MPEG-4, termasuk yang milik Microsoft. Tanpa diragukan lagi, codec MPEG-4 yang paling terkenal adalah DivX. Ia muncul pada saat yang sama dengan MPEG-4 Microsoft, tetapi telah mendapatkan kekuatan dari DivX Networks Inc.

Kita semua tidak mengetahui bahwa melakukan pemeliharaan sistem dapat menyebabkan beberapa hal—yang tak seorang pun dari kita ingin mengalaminya.

Gunung Sarjono



Memelihara Kinerja Windows XP

► Jika komputer Anda tampak lebih lambat dari biasanya, mungkin memang demikian. Komputer kami yang baru satu tahun lebih lambat dibanding pada waktu baru. Seiring dengan waktu, komputer menjadi lebih lambat karena berbagai sebab: file yang tidak teratur, *software* yang tidak diperlukan memakan *resources*, drive jaringan yang tidak digunakan memperlambat *startup*, atau terlalu banyak program yang dijalankan pada waktu *startup*. Masalah serius yang lebih besar juga dapat memperlambat komputer secara dramatis.

Dua hal penting yang perlu dilakukan secara teratur adalah *Disk Cleanup* dan *Disk Defragmenter*. *Disk Cleanup* membersihkan komputer Anda dari bermacam-macam “sampah” yang menumpuk—file *temporary* dari segala macam jenis dan file setup yang lama. *Disk Defragmenter* sedikit lebih jarang, tetapi masih diperlukan sebab file cenderung untuk terus meningkat dari waktu ke waktu.

Kedua permasalahan ini dapat memperlambat sistem, tetapi keduanya mudah diatasi. Yang mengganggu dalam melakukan pemeliharaan sistem adalah bahwa Anda tidak bisa melakukan yang lain-

lain dengan komputer Anda selagi harddisk sedang dibersihkan atau didefragmentasi. Banyak orang menunda pemeliharaan sistem sebab mereka mempunyai pekerjaan yang harus dilakukan, dan mereka bosan melihat proses pemeliharaan dilakukan. Untungnya, dengan Windows XP Anda dapat mengotomatisasi operasi ini. Hanya atur mereka sekali dan lupakan mereka.

Back-up Dulu

Back-up komputer Anda sebelum men-

jalankan *system tools* apapun untuk melakukan *troubleshooting*. Ini bukan peringatan yang berlebihan. Beberapa langkah yang kami sarankan di sini dapat membuat masalah tersembunyi yang sudah ada muncul ke permukaan, yang dapat membuat komputer Anda tidak mau berjalan. Windows XP mempunyai Backup, suatu tool yang membantu Anda melindungi data. Untuk membuka *Backup or Restore Wizard* klik *Start*, pilih *All Programs, Accessories, System Tools*, dan kemudian klik *Backup*.

TIPS

- Lakukan langkah berikut untuk menghapus program yang tidak digunakan:
 1. Klik *Start*, dan kemudian klik *Control Panel*.
 2. Klik *Add or Remove Programs*.
 3. Scroll daftar dan periksa setiap program. Windows XP mencatat seberapa sering Anda menggunakan suatu program dan kapan Anda menjalankannya. Namun, Anda jangan menghapus apapun yang berlabel *Update* atau *Hotfix*, karena mereka meningkatkan keamanan komputer Anda.
 4. Klik program yang tidak lagi Anda butuhkan, klik tombol *Remove*, dan kemudian ikuti *prompt* untuk meng-*uninstall*-nya.

Anda mungkin perlu me-*restart* komputer setelah menghapus program. Setelah komputer di-*restart*, ulangi langkah di atas untuk menghapus program lainnya.

Sebelum membuat perubahan, kami ukur komputer untuk melihat berapa lama untuk *restart*. Dengan demikian, kami bisa mengetahui perubahan mana yang paling signifikan. Komputer kami membutuhkan sekitar 3 menit untuk mati, restart, dan kemudian membuka *e-mail client* dan *browser*. Tentu saja, kami berharap untuk meningkatkan kinerja keseluruhan komputer, tetapi waktu untuk restart paling mudah diukur.

Hapus Program yang Tidak Digunakan

Langkah pertama dalam meningkatkan kinerja komputer Anda adalah dengan menghapus program yang tidak diperlukan. Kami selalu menginstal program baru. Kadang-kadang kami tertarik dengan program baru tersebut dan tetap menggunakannya. Lain waktu, ia tidak melakukan apa yang kami harapkan, dan program tersebut tetap ada dalam komputer, maka ia dapat memakan *resources* dan menurunkan kinerja.

Disk Cleanup

Menggunakan *Disk Cleanup* membantu membebaskan ruang pada harddisk Anda. *Disk Cleanup* mencari harddisk Anda, dan kemudian menampilkan file *temporary*, file *cache* Internet, dan program yang tidak perlu yang dapat dihapus dengan aman.

Disk Cleanup dapat ditemukan dengan dengan mengklik *Start*, *All Programs*, *Accessories*, kemudian *System Tools*, dan kemudian klik *Disk Cleanup*. *Disk Cleanup* akan menampilkan daftar file yang dapat dihapus. Pilih suatu file

TIPS

■ Berikut adalah bagaimana cara mengotomatisasi keseluruhan proses untuk menjalankan *Disk Cleanup* selagi Anda sedang jauh dari komputer:

1. Klik *Run* dari *Start Menu*.
2. Pada kotak *Open*, ketik `cleanmgr /sageset:1`.
3. Klik OK.

Berikutnya, Anda dapat menjadwalkan *Disk Cleanup* untuk dijalankan pada waktu yang diinginkan.

1. Klik *Control Panel*, kemudian klik *System and Maintenance*, dan kemudian klik *Scheduled Tasks*.
2. Klik ganda *Add Scheduled Task* untuk memulai *Scheduled Task Wizard*. Pada daftar aplikasi yang Anda ingin jalankan, klik *Disk Cleanup*, kemudian klik *Next*.
3. Pilih frekuensi untuk tugas—mingguan boleh—dan klik *Next*.
4. Pilih hari dan waktu tugas dijalankan.
5. Masukkan nama dan *password user*. Program akan dijalankan seolah-olah oleh user tersebut. Beri tanda centang (✓) untuk membuka *Advanced Settings* jika sudah selesai.
6. Pada kotak *Run*, tambahkan baris berikut pada bagian akhir: `/sagerun:1` dan kemudian klik OK.

untuk melihat keterangannya. Klik file yang Anda ingin hapus, dan klik OK.

Task Scheduler akan secara otomatis menjalankan *Disk Cleanup* dengan setting yang Anda pilih (Ingatlah untuk meninggalkan komputer tetap menyala!).

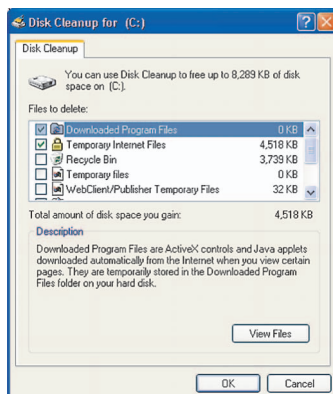
Anda dapat mengatur *Disk Cleanup* untuk menghapus file yang berbeda pada interval yang berbeda dengan menggunakan beberapa *sageset*. Cukup ubah nomornya ke *sageset: 2* atau *sageset: 3* (nomor berapapun dari 0 sampai 65535). Masing-Masing *sageset* dapat mempunyai file yang berbeda. Kemudian Anda dapat membuat jadwal yang terpisah untuk melaksanakan masing-masing tugas dengan menggunakan *sagerun: 2* dan *sagerun: 3* dan seterusnya.

Defragmentasi Komputer Anda

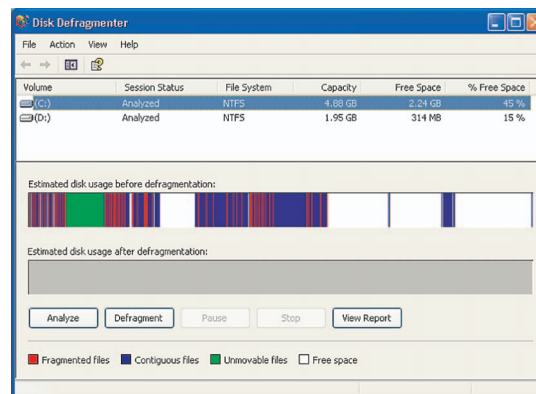
Kami tidak suka artikel koran yang mulai pada halaman depan, tetapi bersambung ke suatu tempat di halaman tengah. Kami bisa lebih cepat membaca artikel tersebut jika dicetak pada halaman yang berurutan seperti artikel majalah. File pada komputer Anda dapat terfragmentasi (terbagi-bagi) seperti surat kabar, atau tidak terfragmentasi (berurutan) seperti majalah.

Seiring dengan waktu, semakin banyak file yang terfragmentasi. Pada waktu file terfragmentasi, komputer membutuhkan waktu lebih lama untuk membacanya karena ia harus melompat ke bagian yang berbeda dari harddisk—sama seperti kami yang membutuhkan beberapa detik untuk menemukan halaman tengah surat kabar. Pada gambar, Anda dapat melihat perbandingan bagaimana komputer membaca file yang tidak terfragmentasi dan terfragmentasi.

Anda juga dapat mendefragmentasi harddisk secara otomatis, meskipun itu tidak perlu sesering membersihkan harddisk. Hanya satu *Disk Defragmenter* yang dapat berjalan pada satu waktu, jadi jika Anda mempunyai beberapa partisi, Anda perlu membuat jadwal yang terpisah untuk masing-masing. Minimum 15% ruang kosong pada harddisk diperlukan oleh *Disk Defragmenter* untuk berjalan.



Gunakan *Disk Cleanup* untuk membersihkan harddisk.



Gunakan *Disk Defragmenter* untuk mengatur file.

TIPS

■ Anda perlu hak administrator untuk mendefragmentasi suatu drive atau volume. Meskipun fragmentasi itu rumit, adalah mudah untuk mendefragmentasi komputer Anda dengan mengikuti langkah berikut:

1. Buka *My Computer*, klik kanan *Local Disk*, dan kemudian klik *Properties*.
2. Pada tab *Tools*, klik *Defragment Now*. Disk Defragmenter akan terbuka.
3. Klik harddisk Anda dan kemudian klik *Defragment*. Disk Defragmenter akan bekerja paling tidak beberapa menit, meskipun kadang-kadang ia membutuhkan beberapa jam.
4. Jika Anda mempunyai beberapa harddisk, ulangi langkah 3 untuk setiap harddisk.

File komputer kami tidak terlalu terfragmentasi, jadi mendefragmentasi mereka tidak mempercepat terlalu banyak. Namun, setelah mendefragmentasi harddisk, Windows dan program lainnya berjalan 20% lebih cepat!

Putuskan Koneksi Jaringan yang Tidak Digunakan

Jika pernah tergabung dalam jaringan dengan beberapa komputer, Anda mungkin berbagi file dengan *mapping* drive jaringan. Drive jaringan memungkinkan satu komputer membaca dan menulis file ke harddisk komputer lain seolah-olah mereka secara langsung terhubung. Kami selalu menggunakan drive jaringan dan bagi kami, mereka mempunyai pengaruh yang cukup signifikan terhadap kinerja.

Permasalahan dengan drive jaringan adalah Windows XP akan mencoba untuk menghubungkan diri ke drive jaringan tersebut pada waktu Windows mulai. Jika komputer *remote* tidak segera merespon, Windows akan menunggu dengan sabar. Di samping itu, beberapa program akan mencoba menghubungkan diri ke drive jaringan pada waktu Anda *browsing* file dan folder. Jika Anda pernah membuka file dan harus menunggu beberapa detik (atau menit!), mungkin karena program tersebut mencoba untuk membuat koneksi jaringan—meskipun jika file yang Anda buka ada di komputer lokal.

Hapus Autostart Program

Langkah berikutnya dalam mengembalikan kinerja komputer Anda adalah dengan mengidentifikasi program yang tidak perlu yang dijalankan secara otomatis. Sering kali program mengonfigurasi diri mereka sendiri untuk berjalan secara *background* sehingga mereka nampak berjalan dengan cepat ketika dibutuhkan. Beberapa dari program ini menampilkan icon pada taskbar

supaya Anda tahu mereka sedang berjalan, sementara yang lain sepenuhnya tersembunyi. *Autostart program* ini mungkin tidak terasa memperlambat komputer pada waktu *startup*, tetapi mereka akan mencuri sejumlah memory dan waktu proses pada waktu komputer Anda berjalan.

Cara lain untuk memeriksa autostart program adalah dengan menggunakan *Autoruns* (<http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml>) tool freeware dari Sysinternals. *Autoruns* menampilkan setiap program yang hendak berjalan secara otomatis dan memungkinkan Anda dengan cepat menghapus *link* ke program tersebut. Banyak entri *autostart* yang merupakan bagian penting dari Windows XP, ter-

masuk *Userinit.exe* dan *Explorer.exe*. Jadi, Anda jangan langsung begitu saja menghapus semua yang tidak dikenal. Sebaliknya, Anda harus melihat setiap entri pada *Startup Application List* Paul Collins (<http://www.sysinfo.org/startuplist.php>) untuk menentukan apakah Anda ingin menjalankannya secara otomatis.

Sebagai contoh, kami menemukan file bernama *nwiz.exe* yang dijalankan secara otomatis. Kami buka *Startup Applications List*, ketik *nwiz* dan menemukan bahwa itu digunakan untuk menentukan pilihan *layout desktop*. Kami ingin tetap menjalankan fungsi ini, jadi kami tidak menghapusnya.

Kami juga menemukan file bernama *Wzqpkick.exe*. Setelah membaca keterangannya pada *Startup Application List*, kami memutuskan bahwa tidak perlu menjalankannya secara otomatis. Kami menghapus link-nya menggunakan *Autoruns* dengan mengklik kanan link dan kemudian mengklik *Delete*. Cara ini cocok untuk pengguna Windows XP tingkat lanjut. Jika Anda tidak yakin apakah program tersebut diperlukan—biarkanlah!

Startup Applications List mungkin menyediakan instruksi untuk menghapus startup program. Jika tersedia, Anda harus mengikuti instruksi itu daripada menghapus link dengan menggunakan *Autoruns*.

TIPS

■ Kami tidak sesabar Windows, dan kami tidak mau menunggu respon dari koneksi jaringan yang tidak digunakan. Untuk mengurangi masalah ini, putuskan koneksi jaringan yang tidak diperlukan dengan melakukan langkah berikut:

1. Buka *My Computer*.
2. Pada menu *Tools*, klik *Disconnect Network Drive*.
3. Pilih drive jaringan yang tidak lagi Anda butuhkan, dan kemudian klik OK.

Setelah memutuskan drive jaringan, komputer kami dapat restart 40% lebih cepat.

TIPS

■ Windows XP mempunyai tool *System Configuration* (*Mscconfig.exe*), yang merupakan cara yang sempurna dalam mengatur proses start up. Untuk menjalankannya:

1. Klik *Start*, klik *Run*, ketik *Mscconfig*, dan kemudian tekan *Enter*.
2. Pada tab *Startup*, Anda akan melihat daftar semua program dan proses yang dijalankan pada waktu Windows XP dimulai.
3. Klik *Apply*, kemudian restart komputer Anda agar perubahannya berlaku.

MEMELIHARA KOMPUTER ANDA

■ Gunakan *best practices* berikut untuk membantu memelihara dan melindungi komputer yang Anda gunakan di tempat kerja. Anda harus menanyakan ke bagian TI untuk mengetahui kebijakan mereka.

1. Instal semua *update* yang diperlukan oleh bagian TI Anda. Dengan tidak menginstal *update* yang diperlukan oleh bagian TI, dapat mengekspos perusahaan Anda terhadap virus dan risiko keamanan lainnya. Beberapa perusahaan bahkan mencegah komputer mengakses jaringan jika *patch* belum diinstal setelah tanggal yang ditentukan. Di samping itu, tanyakan apakah bagian TI ingin Anda menginstal *update* pada office *update* dan Windows *update*. Jika ya, biasakan mengecek kedua situs tersebut secara teratur.
2. Hanya instal program yang berlisensi. Pastikan Anda dan perusahaan Anda mempunyai lisensi atas setiap *software* yang diinstal pada komputer kerja Anda. Perusahaan Anda dapat dituntut karena menggunakan *software* tanpa lisensi. Sebagai contoh, menginstal program yang dibeli oleh teman dapat menimbulkan beberapa masalah. *Software* yang Anda beli lisensinya mungkin sah, tapi periksa sekali lagi lisensi tersebut untuk memastikan. Kadang-kadang, lisensi *software* yang dibeli untuk pengguna rumahan tidak dapat diinstal di tempat kerja.
3. Jangan instal versi *software* yang

berbeda. Walaupun Anda lebih menyukai versi *software* yang digunakan di rumah dibanding di tempat kerja jangan instal pada komputer kerja Anda. Anda dapat mengalami masalah inkompatibilitas dengan rekan kerja dan aplikasi bisnis Anda. Bagian TI Anda juga mungkin tidak dapat melakukan *update* yang diperlukan atau memberikan bantuan teknis.

4. Beritahu bagian TI pada waktu *hardware* tidak bekerja. Memperbaiki sendiri komputer yang rusak dapat menimbulkan lebih banyak masalah. Hasil perbaikan Anda, misalnya, dapat membuat komputer tidak kompatibel dengan jaringan perusahaan. Kebanyakan bagian TI mempunyai *helpdesk* atau program *technical assistance* yang ditujukan untuk pekerjaan seperti ini. Bagian TI mungkin pernah melihat masalah yang sama dan mempunyai solusinya. Membantu bagian TI Anda dalam mencatat masalah komputer yang umum juga dapat membantu mereka dalam menentukan merk komputer yang akan dibeli di masa mendatang.
5. Beritahu bagian TI pada waktu Anda membutuhkan sesuatu. Memberikan permintaan yang beralasan dan waktu yang cukup untuk perencanaan dapat membantu bagian TI dalam merespon permintaan Anda. Jika tidak, Anda mungkin mendapatkan *hardware* atau *software* komputer yang tidak diinginkan—yang dapat menghambat efektivitas Anda di tempat kerja.
6. Jangan *download* program dari situs

Internet yang tidak dipercaya. Dengan men-download program yang mungkin tidak aman, Anda membahayakan semua komputer pada jaringan.

7. Waspada terhadap e-mail yang mencurigakan. Virus diawali melalui e-mail yang disamarkan sebagai file biasa. Jika e-mail yang diterima berasal dari seseorang yang tidak Anda kenal, mempunyai teks yang aneh, atau tampak mencurigakan, hubungi bagian TI Anda. Jika Anda membukanya, besar kemungkinan timbul suatu masalah bagi Anda dan rekan kerja Anda.
8. Gunakan *online support*. Banyak bagian TI yang telah membuat situs *help internal* secara *online* yang dapat memberikan jawaban atas masalah komputer Anda. Setiap hari, *helpdesk* biasanya menerima banyak pertanyaan yang sudah dijawab pada situs ini. Gartner Group, yang melakukan penelitian dan analisis pada industri TI, memperkirakan bahwa pada tahun 2005 telepon ke *support* akan berkurang 50 persen. Para karyawan akan menggunakan fasilitas *help mandiri*—seperti *frequently asked questions* (FAQ) dan panduan *how-to online* untuk membantu mereka memecahkan masalah. Bagi yang menggunakan produk Microsoft, Anda dapat membuka Microsoft Office Online Assistance Center, Microsoft Knowledge Base, dan Windows XP Support Center.

Memperbaiki Masalah yang Lebih Besar

Banyak *user* yang mengalami masalah kinerja yang serius dan tiba-tiba. Suatu hari, komputer mereka baik-baik saja dan besoknya sangat lambat. Masalah seperti ini biasanya disebabkan oleh virus komputer atau *hardware* komputer yang gagal. Saran yang diberikan di sini mungkin tidak akan memperbaiki masalah seperti itu. Lakukan *scan* virus pada komputer Anda.

Jika itu bukan masalahnya, Anda harus menghubungi *technical support*

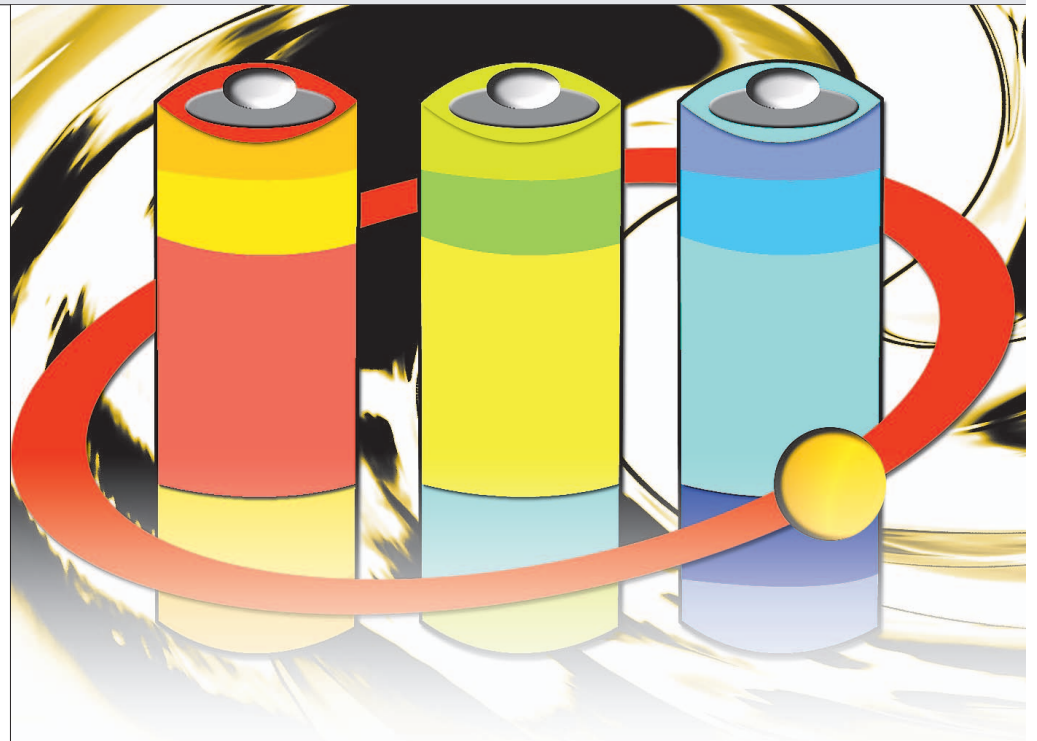
vendor komputer Anda untuk bantuan tambahan. Proses *troubleshooting* untuk masalah seperti ini memerlukan kemampuan untuk memeriksa kinerja komputer berdasarkan proses-proses, dan ini biasanya melibatkan “eliminasi proses” di mana driver, service, dan *hardware* dihapus/diganti satu per satu sampai masalahnya hilang. Besar kemungkinan komputer tidak akan bekerja sama sekali pada tahap tertentu proses ini, jadi ada baiknya mempunyai *support* selama proses ini.

Berbicara tentang kinerja, sering kali berkaitan dengan *tweaking*. Beberapa di antaranya berguna, tetapi kebanyakan jangan digunakan jika Anda tahu pasti apa yang Anda lakukan.

Sebagai contoh, ada *user* yang menganjurkan untuk men-*disable Internet Connection Firewall* untuk meningkatkan kinerja. Meskipun hal itu benar, komputer Anda mudah diserang dari Internet. Kami lebih baik mempunyai komputer yang kinerjanya lebih lambat daripada komputer yang di-*hack!* ■

Dengan teknologi yang masih dikembangkan, saat ini sebuah notebook tidak lagi bekerja hanya 2 sampai 4 jam saja, melainkan dapat terus menyala sampai 20 jam tanpa harus diisi ulang!

Fadilla Mutiarawati



Baterai Masa Depan

► Krisis energi bukan lagi menjadi hal yang baru sekarang. Sudah menjadi berita yang sangat umum bahwa energi yang ada saat ini tidak mencukupi kebutuhan energi yang terus meningkat dari waktu ke waktu. Padahal berbagai sumber energi yang ada dan digunakan saat ini masih dianggap belum sempurna.

Masih banyak kekurangan yang dimiliki oleh sumber energi yang ada. Baik dari segi efektivitas, efisiensi, dan dampak akhir yang diberikan, semuanya masih banyak kekurangannya. Kekurangan dan keterbatasan inilah yang telah banyak mendorong para ilmuwan untuk terus berusaha menemukan jalan keluar. Mencari sumber dan cara baru untuk menghasilkan energi yang lebih baik. Efisien, efektif, dan bersih.

Dari sekian banyaknya sumber energi, batu baterai termasuk bagian yang

memiliki peranan sangat besar. Salah satu sumber energi yang sangat diandalkan oleh perangkat nirkabel yang saat ini mulai menjadi tren dalam masyarakat. Semua perangkat elektronik yang tidak lagi menggunakan kabel, sangat mengandalkan keberadaan batu baterai. Oleh sebab itu, perkembangan teknologi batu baterai telah mencuri perhatian yang tidak kecil dari kalangan produsen CE (*consumer electronic*) dan komputer.

Perhatikan saja batu baterai yang digunakan pada ponsel Anda. Beberapa tahun yang lalu, ponsel hanya menggunakan batu baterai NiMH atau NiCad, namun sekarang hampir seluruh ponsel yang diproduksi sudah menggunakan batu baterai Lithium. Lithium memiliki fisik yang lebih kecil dan ringan dibandingkan NiMH atau NiCad. Selain itu, Lithium juga lebih fleksibel dan tahan lama digunakan.

Namun, kemampuan yang dimiliki oleh Lithium masih dianggap kurang mencukupi. Dengan baterai Lithium, sebuah notebook maksimal dapat bekerja antara 2 sampai 4 jam. Padahal tidak jarang jarak tempuh perjalanan dapat melebihi 4 jam. Sehingga peningkatan daya tahan baterai tentu saja sangat berpengaruh.

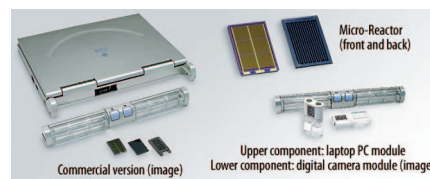
Saat ini, ilmuwan masih terus melakukan penelitian dan percobaan untuk dapat menemukan sebuah batu baterai baru yang dapat menggantikan batu baterai yang ada saat ini. Batu baterai yang tidak hanya memiliki kemampuan lebih, namun juga lebih aman dan bersih pada penggunaannya.

Baterai Masa Depan

Berawal dari krisis yang dialami oleh bahan bakar fosil. Maka saat ini, banyak



Bandingkan Baterai biasa dengan fuel cell dari NEC ini.



Dengan fuel cell, botebook dari Casio ini dapat bertahan selama 20 jam.



Fuel dari MTI untuk PDA. Fuel cell untuk ponsel dari Toshiba.



Notebook dari Fujitsu yang menggunakan *fuel cell*.



Notebook dari Toshiba yang menggunakan *fuel cell*.

ilmuwan berlomba-lomba mencari alternatif bahan bakar. Salah satu di antaranya adalah apa yang disebut dengan *fuel cell*.

Kali pertama dikembangkan, *fuel cell* memang ditujukan untuk pengganti bahan bakar fosil. Namun seiring dengan kemajuan yang dialami oleh *fuel cell* sendiri, saat ini ada juga sudah terdapat *fuel cell* yang dinamakan *micro fuel cell* yang berfungsi sebagai sumber energi perangkat elektronik, seperti ponsel dan komputer serta perangkat lainnya yang membutuhkan bentuk baterai lebih kecil dengan kekuatan tidak terlalu besar.

Salah satu *micro fuel cell* yang paling akhir berhasil dikembangkan saat ini adalah buatan Samsung, yang mampu membuat notebook Anda bekerja selama 10 jam *nonstop* tanpa proses *recharging*.

Samsung tidak sendiri dalam bisnis *micro fuel cell* ini, masih ada produsen lain yang ikut berpartisipasi, seperti Toshiba dan NEC. Pada CeBIT tahun ini, Toshiba telah memamerkan salah satu notebook produksinya Protégé M100 yang dijalankan dengan menggunakan *fuel cell* sebagai sumber energinya. Sedangkan NEC, saat ini tengah mengembangkan sebuah baterai dari *fuel cell* yang dapat dimanfaatkan oleh ponsel tanpa harus men-charge selama satu bulan lebih!

Sebenarnya *fuel cell* sendiri memiliki bahan dasar yang beragam, ada yang menggunakan kombinasi antara hidrogen dan oksigen. Ada juga yang menggunakan bahan dasar methanol. Keduanya memiliki dampak yang berbeda-beda.

Selain bahan dasar yang berbeda, di

antara *fuel cell* juga memiliki kinerja dan dampak yang berbeda juga. Methanol dianggap memiliki kinerja yang paling efektif. Namun berhubung methanol bersifat *toxic* (beracun), maka residu yang dihasilkannya pun sangat berbahaya.

Residu yang dihasilkan oleh methanol berupa gas karbon yang dapat menimbulkan efek rumah kaca pada lapisan bumi. Sedangkan hidrogen yang tidak memiliki efektivitas sebesar methanol, hanya mengeluarkan air (H_2O) sebagai residunya. Oleh sebab itu, *fuel cell* hidrogenlah yang saat ini paling banyak dikembangkan oleh ilmuwan karena dianggap lebih ramah lingkungan.

Cara Kerja

Seperti yang dikatakan sebelumnya bahwa pada *fuel cell* hidrogen, hidrogen, dan oksigenlah yang digunakan sebagai bahan bakarnya. Reaksi antara keduanya mampu menghasilkan energi listrik dan air.

Seperti halnya sebuah baterai yang memiliki bagian-bagian penting seperti anoda dan katoda, *fuel cell* juga demikian. Yang berperan sebagai anoda adalah hidrogen (*fuel*) dan yang berperan sebagai katoda adalah oksigen (oksidan). Sedangkan yang berperan sebagai katalisatornya adalah bubuk platina yang terbungkus oleh kertas karbon.

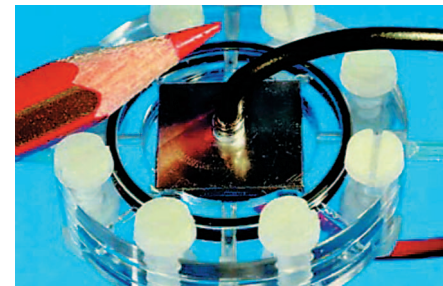
Pada saat hidrogen (H_2) yang diberikan tekanan terdorong pada anoda, maka hidrogen akan melewati katalisator yang akan membuatnya terionisasi menjadi (ion H^+) dan elektron. Kemudian proton dan elektron akan mengalir menuju katoda dan bereaksi dengan zat O_2 yang ada di sana mem-

bentuk sebuah zat yang dinamakan H_2O atau yang biasa kita kenal dengan air. Namun, sebelum proton dan elektron mencapai katoda kedua zat ini akan terlebih dahulu melewati dua jalur berbeda. Elektron melewati sebuah sirkuit listrik, agar sempat membentuk arus listrik terlebih dahulu. Sedangkan proton mengalir melalui elektrolit yang tidak bersifat konduktor.

Tegangan listrik searah (DC) yang dihasilkan oleh satu reaksi ini memang hanya 0,7 Volt. Namun, bukan berarti sebuah *fuel cell* hanya mampu menghasilkan tegangan 0,7 Volt saja. Sebab dalam satu sistem yang lengkap, tidak hanya menggunakan satu lapis *fuel cell* saja, melainkan banyak lapisan *fuel cell* yang kemudian disebut *fuel cell stack*. Sehingga jumlah tegangan yang dihasilkan dapat bertambah. Bahkan keseluruhan daya listrik yang diperoleh dari *fuel cell* ini ada yang dapat mencapai 20 Watt. Lumayan, bukan?

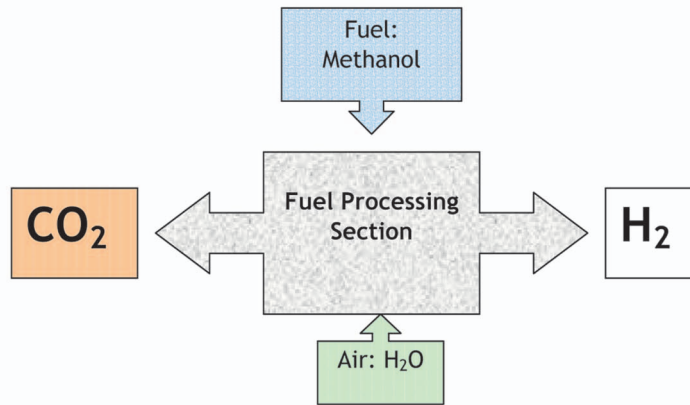
Pro dan Kontra

Menggunakan hidrogen sebagai bahan dasar sebuah baterai memang sangat



Dengan bantuan teknologi Nano, bentuk *fuel cell* nantinya dapat menandingi besar ujung pensil Anda.

Ada tambahan proses kerja pada DMFC, dimana Methanol akan diproses dahulu untuk menghasilkan Hydrogen.



efektif. Namun sayangnya, bahan bakar ini memiliki beberapa kelemahan yang membuatnya sampai saat ini belum umum digunakan. Hidrogen selain sangat sulit diperoleh juga sangat mudah meledak, sehingga untuk memasangnya pada perangkat *mobile* Anda yang banyak berpindah dianggap sangat riskan.

Oleh sebab itu, muncullah gagasan untuk menggunakan methanol sebagai bahan dasar *fuel cell*. Fuel cell ini pun dinamakan DMFC, yaitu singkatan dari *Direct Methanol Fuel Cell* yang artinya fuel cell tersebut menggunakan methanol secara langsung sebagai bahan bakarnya.

Keberadaan methanol sendiri bukanlah untuk menggantikan hidrogen seluruhnya. Methanol pada fuel cell justru digunakan untuk direaksikan dengan air yang hasilnya justru akan menghasilkan zat hidrogen. Membawa-bawa methanol tidak terlalu berbahaya seperti layaknya hidrogen. Begitu pula dengan proses perolehan hidrogennya, dengan cara ini dianggap lebih aman dibandingkan jika harus menenteng-nenteng hidrogen ke mana-mana.

Sayangnya, seperti yang tadi sempat diungkapkan dalam proses mendapatkan hidrogen inilah reaksi methanol dengan air juga akan menghasilkan zat lain, yaitu karbon. Sebuah zat yang sangat berbahaya bagi lingkungan. Namun, berhubung kebutuhan akan sumber daya yang mampu bertahan lama sudah sangat mendesak, maka sebelum fuel

cell yang lebih ramah lingkungan ditemukan, DMFC pun sudah mulai diproduksi.

Di samping itu, hidrogen yang dihasilkan melalui DMFC ini dianggap lebih efektif ketimbang fuel cell berbahan bakar hidrogen langsung. Sebab pada saat reaksi kimia terjadi ketika methanol bertemu dengan air, maka jumlah electron yang mengalir tidak lagi $2e^-$, melainkan $6e^-$. Untuk lebih jelasnya mengenai reaksi kimia ini, Anda dapat melihat pada rumus yang disediakan.

Air yang akan bereaksi dengan methanol tidak perlu diisi secara manual.

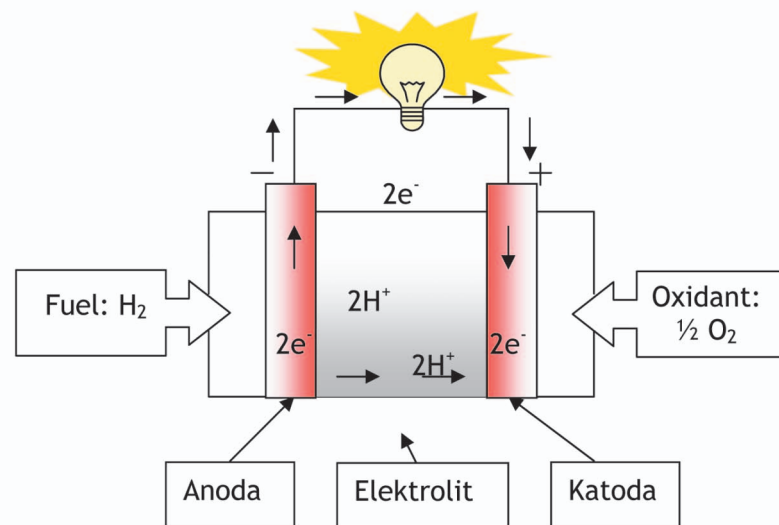
Seperti yang diketahui bahwa pada reaksi fuel cell, air telah menjadi hasil akhir. Air inilah yang nantinya akan diputar kembali, direaksikan dengan methanol untuk memperoleh hidrogen.

Fuel cell yang menggunakan methanol dengan yang menggunakan hidrogen memiliki ukuran yang berbeda. Lebih besar fuel cell yang menggunakan bahan bakar methanol dibandingkan dengan fuel cell yang menggunakan langsung bahan bakar hidrogen. Sebab pada fuel cell berbahan bakar methanol diperlukan sebuah sistem tambahan untuk memproses zat methanol tersebut.

Tahapan tersebut dinamakan proses *fuel processing section*. Proses ini memiliki tempatnya sendiri, bukan pada anoda. Dalam anodanya sendiri zat yang masuk adalah $3H_2$. Kemudian proses yang terjadi antara anoda dengan katoda sama halnya dengan yang terjadi dalam fuel cell berbahan bakar hidrogen langsung. Hanya saja, konsentrasinya agak sedikit berubah. O_2 yang digunakan tidak lagi $\frac{1}{2}$ melainkan 1 !. Dan H_2O (air) yang dihasilkan pun bernilai $3H_2O$. Yang artinya lebih banyak air yang dihasilkan.

Sedangkan Karbon yang juga dihasilkan melalui proses ini akan terbuang ke udara langsung. Inilah yang menjadi alasan mengapa DMFC dapat merusak lingkungan.

Prinsip kerja Fuel Cell berbahan bakar Hydrogen langsung



Sampai saat ini, justru fuel cell berbahan bakar methanol-lah yang paling banyak dikembangkan dan diproduksi oleh perangkat portabel. Salah satunya adalah Toshiba yang belum lama ini memperkenalkan salah satu notebooknya yang menggunakan baterai fuel cell yang berbahan bakar methanol.

Notebook tersebut ada dua macam, yang pertama dengan jumlah zat methanol cair sebanyak 50 ml dapat bertahan selama 5 jam dan yang kedua dengan zat methanol cair sebanyak 100 ml dapat bertahan selama 10 jam tanpa proses *recharge*. Jauh lebih lama ketimbang menggunakan baterai biasa yang paling lama hanya bertahan 4 jam.

Selain mencoba untuk memproduksi Notebook dengan DMFC, Toshiba juga mencoba untuk memproduksi DMFC untuk digunakan pada ponsel.

Pembuatan baterai dari DMFC tidak hanya dilakukan oleh Toshiba, NEC juga memproduksi DFMC dengan ukuran yang sangat kecil. lihat saja pada gambarnya, jika dibandingkan dengan baterai AA, maka DMFC buatan NEC tidak jauh berbeda.

Sedangkan untuk PDA, salah satu baterai fuel cell methanol yang kini dapat digunakan adalah produksi MTI

BATERAI DARI JERUK LEMON

■ Ada hal yang menarik menyangkut baterai sebagai sumber daya listrik. Dan mungkin hal ini sudah diketahui oleh sebagian besar dari Anda. Bahwa energi listrik selain dapat diperoleh dari bahan nonorganik, juga dapat diperoleh dari bahan organik, seperti buah misalnya.

Salah satu buah yang paling sering digunakan untuk menghasilkan energi listrik adalah jeruk lemon. Tidak percaya? Anda dapat mencobanya sendiri di rumah. Caranya dengan menusukkan satu lempengan timah dan satu lempengan tembaga secara berjajar tanpa saling bersentuhan. Kemudian pada ujung masing-masing lempengan dijepit dengan kabel yang menggunakan penjepit. Jika kedua kabel ini disatukan, maka akan ada listrik yang mengalir di antara kedua kabel tersebut. Dan besarnya tegangan listrik yang mengalir ini dapat mencapai 1 Volt. Nilai yang cukup untuk menjalankan sebuah jam digital sederhana. Jika tidak percaya, Anda dapat mencobanya dan mengukurnya dengan bantuan Voltmeter di rumah.

Lemon seperti halnya sebuah batere mengandung asam yang bersifat elektrolit yang dapat menghasilkan energi listrik. Ketika reaksi kimia antara asam pada lemon dan lempengan-lempengan berlangsung, pada saat itulah energi listrik dapat dihasilkan.

Menarik, bukan? Ternyata selain memberikan vitamin C yang besar, jeruk juga dapat dijadikan sumber energi listrik.



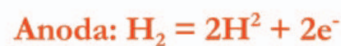
MicroFuel Cell, yaitu Mobion. Mobion sangat kecil dan tipis sehingga selain pada PDA, fuel cell ini juga dapat digunakan pada sebuah *smart label*.

Bentuknya yang sangat tipis tidak akan terlalu mengganggu atau menyulitkan label itu sendiri.

Mungkin untuk perusahaan-perusahaan yang memproduksi notebook/laptop atau ponsel, keterlibatannya dalam dunia baterai tidak asing lagi. Lain halnya dengan perusahaan seperti Casio. Hebatnya, meskipun Casio lebih banyak dikenal masyarakat melalui produk seperti jam tangan dan CE (*Consumer Electronic*), ternyata Casio juga mencoba untuk ikut ambil andil dalam kemajuan teknologi fuel cell ini. Dengan sebuah notebook yang khusus diciptakan untuk percobaan ini, Casio berhasil membuat sebuah DMFC yang mampu membuat notebook-nya bekerja selama 20 jam tanpa proses recharge. Casio tidak hanya memproduksi DMFC untuk notebook saja, bahkan ia juga memproduksi DMDC untuk kamera digital dan PDA-nya.

Mungkin satu atau dua tahun lagi teknologi baterai portabel yang menggunakan fuel cell sudah dapat dinikmati oleh masyarakat. Jauh lebih cepat daripada kendaraan yang sebelumnya menjadi awal penelitian fuel cell. ■

Proses Kimia yang berlangsung dalam Fuel Cell:



Jika menggunakan Methanol, maka reaksi kimianya menjadi:



E-book memang dikembangkan dari aplikasi *document viewer*. Namun biar bagaimanapun, antara e-book dengan *document viewer* tidak sama, baik dari segi layar maupun aplikasi.

Fadilla Mutiarawati



E-Book Berbeda dengan Document Viewer

► Sebuah *document viewer* biasanya digunakan untuk mempermudah seseorang dalam melihat sebuah dokumen. Dan keberadaannya tidak membutuhkan teknologi layar yang tinggi. Sebab dari awalnya, keberadaan aplikasi ini bukanlah untuk melihat sebuah dokumen yang panjang dan rumit seperti buku, melainkan hanya untuk mempermudah seseorang dalam melihat sebuah dokumen digital yang biasanya tidak terlalu banyak.

Dengan *document viewer*, kita dapat menggabungkan beberapa dokumen mulai dari teks, tabel, sampai gambar tanpa harus membuka aplikasi berbeda. Serta dengan *document viewer* data yang dibuat pun tidak akan berpindah tempat. Di samping itu dengan dokumen viewer, bobot dokumen juga akan mengalami kompresi. Sehingga dapat lebih *mobile* dibanding jika harus mengirimkan dokumen yang terpisah-pisah.

Sedangkan e-book, sesuai dengan namanya e-book (*electronic book*) adalah versi digital dari sebuah buku.

Banyaknya data dalam e-book jauh lebih panjang dari dokumen digital biasa. Sehingga untuk membacanya dibutuhkan kenyamanan tersendiri, baik dari segi *hardware*-nya maupun aplikasinya.

Keduanya memang memiliki perangkat dan aplikasi yang serupa, namun pada penerapannya keduanya sangat berbeda. Baik dari peralatan yang digunakan maupun aplikasi yang dibutuhkan. Perbedaan mendasar terletak pada layar yang digunakan oleh keduanya serta program yang dipakai.

Layar

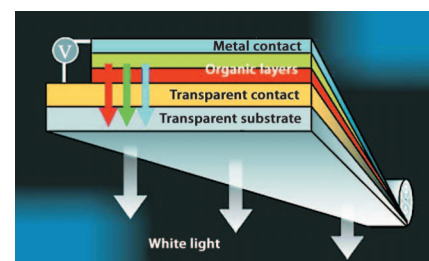
Berbeda dengan *document viewer* yang tidak memerlukan layar yang terlalu canggih. Sebab durasi membaca sebuah dokumen tidaklah selama membaca buku. Oleh sebab itu pula aplikasi ini dikenal dengan sebutan *document viewer*.

Meskipun sekarang sudah banyak e-book yang dibaca dengan menggunakan komputer, PDA, atau ponsel, namun tetap

saja hal tersebut dianggap kurang proporsional untuk dilakukan. Mengingat isi buku sangat panjang dan teknologi layar yang ada saat ini pada masing-masing peralatan tersebut belum dianggap memiliki nilai kenyamanan yang sama dengan kertas pada buku atau koran.

CRT. Meskipun keberadaannya masih terus dikembangkan dan produksinya masih terus meningkat. Namun CRT tidak mampu menjadi layar utama untuk e-book, mengingat CRT tidak cukup fleksibel untuk dijadikan alat baca.

Selain CRT, LCD adalah pilihan utama. LCD memiliki bentuk fisik yang lebih



Susunan dalam sebuah OLED.

ramping, ringan, dan mengonsumsi daya lebih sedikit dibandingkan CRT. Namun resolusi yang dimiliki LCD belum sebaik CRT. Selain itu, hal lain yang menjadi kelemahan LCD adalah *angle view*-nya yang lebih sempit dibandingkan CRT.

Dan bila Anda membaca dengan layar LCD di bawah sinar matahari, maka gambar maupun tulisan tidak akan dapat terlihat dengan jelas.

Melalui teknologi LCD, ada satu lagi layar yang diproduksi secara massal dan saat ini sedang sangat digemari, yaitu layar plasma. Namun, layar plasma dianggap juga belum mampu memenuhi kebutuhan mata untuk membaca e-book. Sampai akhirnya ditemukan sebuah teknologi baru yang dinamakan OLED.

Struktur OLED terdiri atas lapisan kaca yang dilapisi dengan oksida timah-indium yang berfungsi sebagai anoda. Di atas lapisan oksida terdapat lapisan organik dari *aromatic diamine* yang tebalnya 750 angstrom (75 nm), lapisan *light-emitting* terbuat dari senyawa metal kompleks misalnya *8-hydroxy-quinoline aluminium*, dan lapisan katoda yang terbuat dari campuran logam magnesium dan perak (dengan perbandingan atom 10:1). Konstruksi struktur lapisan seluruhnya tidak lebih dari 500 nm.

OLED adalah singkatan dari *Organic Light Emitting Diode*. Dari namanya sudah dapat diketahui bahwa OLED terbuat dari lapisan organik yang memancarkan cahaya. Lapisan paling atas yang berfungsi sebagai anoda dari sebuah OLED adalah Oksida Timah Indium, lalu diikuti oleh lapisan organiknya dari *aromatic diamine*, diikuti dengan lapisan pemancar cahayanya, kemudian sebagai lapisan terakhir yaitu lapisan yang berfungsi sebagai katoda yang terbuat dari campuran magnesium dan perak.

Keseluruhan konstruksi OLED hanya sekitar 500 nm. Yang artinya sangat tipis sekali. Oleh sebab itu, OLED dapat digulung seperti layaknya selebar kertas.

Jika LCD memiliki *angle view* sebesar 10 derajat saja, maka OLED mampu memberikan *angle view* sebesar 160 derajat. OLED juga jauh lebih tipis dan

ringan, sehingga lebih fleksibel dan lebih mungkin untuk digunakan untuk membaca e-book. Konsumsi daya OLED pun tidak terlalu besar, sekitar 1/3 dari yang digunakan oleh LCD. Cukup hemat, bukan? Oleh sebab itu, OLED lebih fleksibel dan lebih mungkin untuk digunakan pada e-book.

Dan berhubung semua bahan penyusun OLED lebih murah dari pada cairan pada layar LCD atau tabung pada layar CRT, maka harga OLED pun dapat lebih murah dibandingkan LCD maupun CRT.

Aplikasi

Kebutuhan masyarakat yang sangat besar akan keberadaan *document viewer* telah membuat aplikasi ini tersedia secara gratis. Salah satu dokumen viewer yang dapat di-*download* secara cuma-cuma adalah Adobe Acrobat Reader yang berformat pdf. Banyaknya para pengguna format dan aplikasi ini juga telah mendorong format pdf sebagai standar format untuk document viewer.

Aplikasi yang digunakan sebagai document viewer ini jugalah yang telah menjadi inspirasi bagi aplikasi yang digunakan oleh e-book sebagai *reader*-nya. Oleh sebab itu, tampilan sebuah reader pada e-book tidak jauh berbeda dengan Acrobat Reader yang biasa digunakan sebagai document viewer.

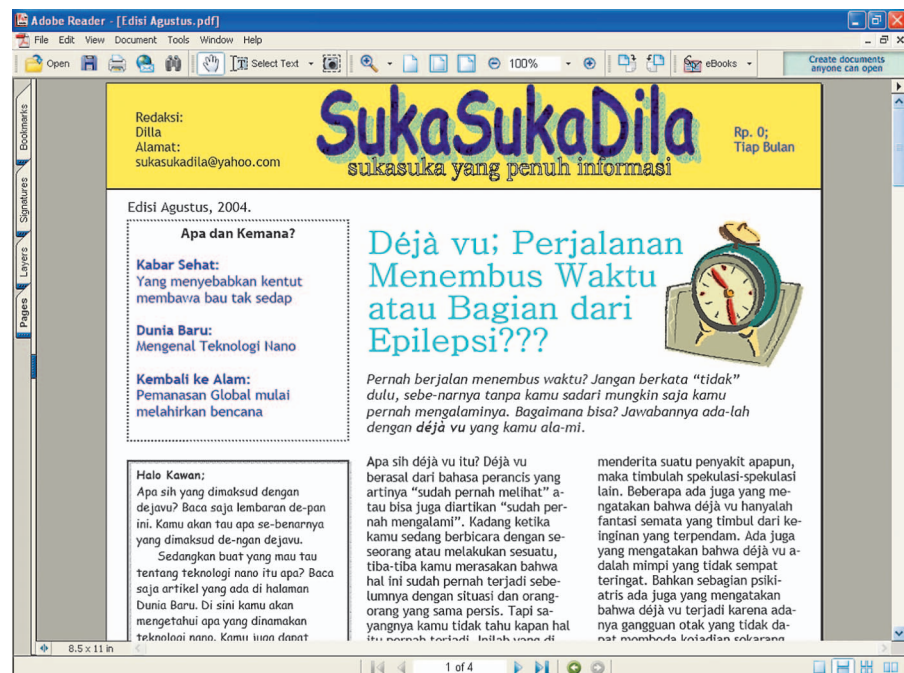
Sama seperti halnya sebuah document viewer, pada sebuah reader yang digunakan untuk e-book juga dapat menampilkan teks, tabel, dan gambar. Namun, ada beberapa hal yang membuat pdf tidak digunakan sebagai format standar e-book.

Tingkat Keamanan Beragam

Namun, satu hal yang tidak dimiliki oleh sebuah *document viewer* adalah tingkat keamanan yang tinggi, yang melindungi hak cipta dari e-book itu sendiri. Tingkat keamanan ini juga yang akan menghalangi seseorang untuk meng-*copy*, mencetak, mem-*forward*, atau bahkan mengedit isi dari e-book tersebut.

Sebenarnya pada aplikasi pdf terdapat beberapa jenis keamanan yang dibutuhkan oleh e-book. Namun, keberadaannya masih dianggap kurang lengkap. Pada pdf, Anda memang tidak akan dapat mengedit isi dokumen, sebab memang pdf hanya berfungsi sebagai *viewer* bukan file editing. Selain itu, ada juga beberapa jenis keamanan lain seperti tidak dapat meng-*copy* bagian dari isi dokumen atau tidak dapat mencetak dokumen.

Sedangkan untuk menduplikasi file-nya sendiri atau bahkan mengirimkan kepada orang lain, dengan pdf masih dapat dilakukan. Kegiatan ini tentu saja



Pdf kurang cocok untuk dijadikan alat membaca e-book.

akan merugikan penerbit jika pada e-book tidak dihilangkan. Seseorang bisa hanya membeli satu buah e-book saja lalu mengirimkan copy-nya pada orang lain yang ingin membaca e-book yang sama tanpa si pembaca harus membayar.

Tingkat keamanan pada e-book masih lebih beragam. Ada juga e-book yang hanya memberikan hak kepada si pemilikinya untuk memasang e-book pada satu perangkat komputer saja. Atau ada juga e-book yang dapat di-copy dengan jumlah tertentu. Berbagai macam tingkat keamanan inilah yang menjadikan aplikasi e-book juga beragam.

Sistem keamanan pada e-book dinamakan juga DRM (*Digital Right Management*). Satu hal lagi yang sangat membedakan sistem keamanan antara pdf sebagai document viewer dengan e-book adalah DRM tadi. DRM berbasiskan sebuah server. Ini artinya, sistem keamanan yang dimiliki oleh e-book berbasiskan server data dari e-booknya itu sendiri. Sedangkan sistem keamanan

untuk document viewer seperti pdf tidak membutuhkan server sebagai bagian dari system kemanannya.

Sampai saat ini, memang belum terdapat sebuah aplikasi yang dapat memberikan fasilitas keamanan yang lengkap. Setiap aplikasi masih memiliki formatnya masing-masing. Dan setiap aplikasi memberikan hak yang berbeda-beda pada pembacanya.

Mengapa Tidak pdf Saja yang Dikembangkan

Mengapa tidak mengembangkan teknologi yang sudah lebih dulu hadir? Mungkin pertanyaan ini sempat terpikir oleh para *user* yang merasa direpotkan harus menginstal aplikasi tambahan untuk membaca e-book. Padahal pada komputer atau PDA-nya sudah terpasang sebuah *reader* berupa Acrobat Reader.

Ini adalah pertanyaan yang wajar. Mengingat antara aplikasi reader untuk e-book memang tidak jauh berbeda dari aplikasi Acrobat Reader, baik dari segi








tampilan maupun tingkat keamanan. Namun ternyata, ada satu bagian dari pdf yang tidak terlalu disadari oleh umum yaitu efektivitas acrobat reader sendiri sebagai aplikasi reader untuk e-book.

Acrobat Reader sebagai document viewer ternyata lebih berorientasi pada ukuran kertas 8,5x11 inci, yang memang lebih banyak digunakan pada pembuatan dokumen dengan komputer. Sedangkan, buku sendiri memiliki ukuran yang lebih kecil, ukuran yang lebih nyaman.

Meskipun demikian, bukan berarti e-book merupakan teknologi yang dengan sendirinya hadir. Justru salah satu teknologi yang mendukung perkembangan e-book sendiri adalah teknologi document viewer seperti PDF-lah yang mana telah lebih dulu hadir.

Bagi Anda yang berkenan untuk membaca e-book saat ini, berikut kami sertakan daftar aplikasi e-book yang dapat dipilih sesuai dengan perangkat yang digunakan. ■























Jenis Perangkat dan E-booknya.

IMAGE	E-BOOK FORMAT	BERAT	UKURAN	LAYAR
	MobiPocket	6,5 oz	5,17" x 3,39" x 0,67"	240 x 200 pixel LCD
	Gemstar eBook	17 oz	Largish	4,75" x 3" Monochrome Back lit Touch screen
	Palm Reader MobiPocket	1,1 lbs	7,44" x 3,74" x 1,34"	6,5 in color LCD display 640 x 240 px on screen
	Palm Reader MobiPocket	5,4-6,9 oz	Smallish	About 3"x4". Ada yang berwarna ada yang tidak berwarna
	hiebook	8,8 oz	115,4 x 146 x 17 mm	Back lit 480 X 320 px touch screen LCD display
	Palm Reader MobiPocket	4-6 oz	4,82" x 3,1" x 87"	LCD dengan backlight
	Microsoft Reader MobiPocket	6-16 oz	Tergantung dari perangkatnya	Reflective atau Transflective LCD, 16+ colors

Persyaratan Sistem Tiap Perangkat.

PERANGKAT	OPERATING SYSTEM	RAM	DISK SPACE	KONEKSI
Franklin eBookMan	PC486 atau lebih tinggi dengan sistem operasi Windows® NT 4.0, Windows® 98, atau Windows® 2000	32 MB RAM (dianjurkan)	50 MB	USB port
Gemstar eBook	N/A	N/A	N/A	USB port untuk koneksi ke PC dan Infrared port (IrDA 1.0)
Handheld PC	Windows	N/A	N/A	RS232C serial port, 115 Kbps IrDA port, 115 Kbps RJ11 modem port (khusus hp jornada 720)
Handspring Visor	Windows 98, Me and 2000 atau Windows 95, NT 4.0 dengan serial port atau Macintosh System 8.5 ke atas	8 MB RAM minimum (dianjurkan 16 MB)	25 MB	USB Cradle
hiebook	Windows	N/A	N/A	USB Cradle
Palm	PC with Windows 98, 2000 atau Me, Macintosh dengan PowerPC prosesor dan Mac OS 8.5.1 ke atas	5 MB free RAM untuk Macintosh	30 MB	USB Cradle
Pocket PC	Tergantung pada perangkatnya	Tergantung pada perangkatnya	Tergantung pada perangkatnya	USB Cradle

Perbedaan Setiap Format.

FORMAT	ADVANTAGES	READER SOFTWARE	NAVIGATION	IMAGES	PLATFORMS
	Dapat dicetak single atau double page view, cross platform compatibility Khusus digunakan untuk e-book		Library, Table of contents, Chapter links, bookmarkable	Ya	Windows, Macintosh, Linux, Unix, Palm
	Khusus digunakan untuk e-book dan beberapa aplikasi tambahan lainnya		Library, Table of contents, bookmarks	Ya	Gemstar & Rocket eBook devices
	Khusus digunakan untuk e-book dan beberapa aplikasi tambahan lainnya		Library, Table of contents, bookmarks	Ya	hiebook devices
	Mudah digunakan, dapat dibaca dengan aplikasi browser		Hypertext links	Tidak	Windows, Macintosh, Linux, Unix, Palm, Pocket PC, eBookMan
	Mudah digunakan, hanya membutuhkan aplikasi Internet Explorer		Hypertext links	Ya	Windows Computers
	Menggunakan teknologi ClearType Display. Sangat mirip dengan buku, ada bookmark dan notasi		Library, Table of contents, Chapter links, bookmarkable	Ya	Windows Computers, Pocket PC
	Sudah sangat familiar, dapat dicetak dan ukuran teksnya dapat diubah		Hypertext links	Ya	Windows, Macintosh
	Dapat digunakan pada semua PDA		Library, Table of contents, Chapter links, bookmarkable	Ya	Palm, Pocket PC, eBookMan
	Sangat sederhana, dapat dibaca di mana saja, dapat juga dicetak	 	N/A	Tidak	Windows, Macintosh, Linux, Unix, Palm, Pocket PC, eBookMan
	Sangat cocok untuk PDA	 	Library, Table of contents, Chapter links, bookmarkable	Tidak	Palm OS, Pocket PC, Handheld PC, Windows CE