REVIEW PROPOSAL RANCANG BANGUN SISTEM MONITORING RUANGAN

MENGGUNAKAN WEBCAM BERBASIS OPENWRT

Dosen Pengampu : Bapak Triawan Adi Cahyanto, M.Kom

Disusun oleh:

Dwi Rahmad Yanuar Rizki R.T.

1410652018

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek pentingdari sebuah system informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi.Seringkali masalah keamanan berada di urutan kedua,atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan [11]. Buku ini diharapkan dapat memberikan gambaran dan informasi menyeluruh tentang keamanan sistem informasi dan dapat membantu para pemilik dan pengelola sistem informasi dalam mengamankan informasinya.

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "information-based society". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Dahulu, jumlah komputer sangat terbatas dan belum digunakan untuk menyimpan hal-hal yang sifatnya sensitif. Penggunaan komputer untuk menyimpan informasi yang sifatnya classified baru dilakukan di sekitar tahun 1950-an.

Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dalam development, algoritma-algoritma dan teknik-teknik yang digunakan untuk

menghasilkan produk tersebut. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima.

Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai berbondong-bondong membuat LAN untuk system informasinya dan menghubungkan LAN tersebut ke Internet. Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (security hole) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi.

Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik

DASAR-DASAR KEAMANAN SISTEM INFORMASI

Sebelum melangkah lebih jauh kepada hal yang praktis dalam pengamanan sistem informasi, ada baiknya kita pelajari dasar-dasar (principles) dan teori-teori yang digunakan untuk pengamanan sistem informasi. Kriptografi, enkripsi, dan dekrtipsi (baik dengan menggunakan private-key maupun dengan menggunakan public-key) akan dibahas secara singkat di dalam bab ini. Bagi yang ingin mendalami lebih jauhmengenai kriptografi, disarankan untuk membaca buku-buku yang digunakan sebagai referensi pada bab ini karena bahasan kriptografi bisa menjadi satu buku tersendiri.

David Khan dalam bukunya The Code-breakers membagi masalah pengamana informasi menjadi dua kelompo; security dan intelligence. Security dikaitkan dengan pengamanan data, sementara intelligence dikaitkan dengan pencarian (pencurian, penyadapan) data. Keduanya sama pentingnya. Bagi sebuah

perusahaan, biasanya masalah pengamanan data yang lebih dipentingkan. Sementara bagi militer dan intel, masalah penyadapan data merupakan hal yang penting juga karena ini menyangkut keamanan negara. Hal ini menimbulkan masalah baru seperti masalah privasi dan keamanan negara, masalah spy versus spy.

Security	Intelegensi
Signal security: steganography, traffic security (call sign changes, dummy message, radio silence), cryptography	**Signal intelligence:** intercepting & direction finding, traffic analysis, cryptanalysis
Electronic security: emission security (shifting radar frequency), counter-countermeasures (looking through jammed radar)	**Electronic intelligence:** electronic reconnaissance (eavesdroping on radar emission), countermeasure (jamming, false radar echoes)

Majalah IEEE Spectrum bulan April 2003 menceritakan tentang penyadapan internasional yang dilakukan oleh beberapa negara yang dimotori oleh Amerika Serikat, Inggris, dan Australia. Penyadapan ini dilakukan secara besar-besaran di udara, darat, dan laut. Jadi, masalah penyadapan informasi negara bukan isapan jempol lagi. Ini sudah menjadi informasi yang terbuka.

Melakukan penyadapan dan mengelola data yang disadap bukan hal yang mudah. Apalagi jika volume dari data tersebut sangat besar. Masalah itu menjadi fokus bahasan dari IEEE Spectrum edisi April 2003 tersebut. Bagaimana melakukan penyadapan terhadap pembicaraan orang melalui telepon? Bagaimana mendeteksi kata-kata tertentu? Perlukan semua hasil sadapan disimpan dalam database? Seberapa besar databasenya? Bagaimana proses data mining, pencarian informasi dari database tersebut. Masih banyak pertanyaan-pertanyaan lain yang belum terjawab secara teknis.

Pengamanan data dapat dilakukan dengan dua cara, yaitu steganography dan cryptography . Biasanya kita hanya familier dengan cara yang terakhir saja. Namun steganografi juga memiliki banyak manfaat.

Steganografi

Pengamanan dengan menggunakan steganografi membuat seolah-oleh pesan rahasia tidak ada atau tidak nampak. Padahal pesan tersebut ada. Hanya saja kita tidak sadar bahwa ada pesan tersebut di sana. Contohsteganografi antara lain:

- Di jaman perang antara Yunani dan Persia, pesan rahasia disembunyikan dengan cara menuliskannya di meja (mebel) yang kemudian dilapisi dengan lilin (wax). Ketika diperiksa, pesan tidak nampak. Akan tetapi sesampainya di tujuan pesan tersebut dapat diperoleh kembali dengan mengupas (kerok) lilin yang melapisinya.
- Di jaman Histalaeus, pesan disembunyikan dengan cara membuat tato di kepala budak yang telah digunduli. Kemudian ditunggu sampai rambut budak tersebut mulai tumbuh baru sang budak dikirimmelalui penjagaan musuh. Ketika diperiksa di pintu gerbang lama memang sang budak tidak membawa pesan apa-apa. Sesampainya di tujuan baru sang budak dicukur oleh sang penerima pesan untuk dapat dibaca pesannya. (Bagaimana cara menghapus pesannya? Sadis juga.).
- Pesan rahasia dapat juga dikirimkan dengan mengirimsurat pembaca ke sebuah surat kabar. Huruf awal setiap kalimat (ataubisa juga setiap kata) membentuk pesan yang ingin diberikan. Cara lain adalah dengan membuat puisi dimana huruf awal dari setiap baris membentuk kata-kata pesan sesungguhnya.
- Hal yang sama dapat dilakukan dengan membuat urutan gambar buah dimana pesan tersebut merupakan gabungan dari hurufawald dari nama buah tersebut.
- Pengarang Dan Brown dalam buku novelnya yang berjudul “The Da Vinci Code” [4] memberikan pesan di sampul bukunya dengan membuat beberapa huruf dalam cetakan tebal (bold). Jika disatukan, huruf-huruf yang ditulis dalam cetakan tebal tersebut membuat berita yang dimaksud. (Silahkan lihat pada gambar berikut. Apa isi pesannya?).

- Di dunia digital, steganografi muncul dalam bentuk digital watermark, yaitu tanda digital yang disisipkan dalam gambar (digital image) atau suara. Hak cipta (copyright) dari gambar dapat disisipkan dengan menggunakan high-bit dari pixel yang membentuk gambar tersebut. Dasar-Dasar Keamanan Sistem Informasi 32 Keamanan Sistem Informasi Berbasis Internet - Budi Rahardjo Gambar terlihat tidak berbeda - karena kemampuan (atau lebih tepatnya ketidakmampuan) mata manusia yang tidak dapat membedakan satu bit saja - akan tetapi sebenarnya mengandung pesan-pesan tertentu.
- Steganografi juga muncul dalam aplikasi digital audio, seperti misalnya untuk melindungi lagu dari pembajakan. Contoh lain adalah menyisipkan informasi sudah berapa kali lagu tersebut didengarkan. Setelah sekian kali didengarkan, maka pengguna harus membayar sewa lagu. (Meskipun pendekatan ini masih bermasalah.)

Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (Cryptography is the art and science of keeping messages secure. [45]) "Crypto" berarti "secret" (rahasia) dan "graphy" berarti "writing" (tulisan) [3]. Para pelaku atau praktisi kriptografi disebut cryptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.

Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption). Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "encipher". Proses sebaliknya, untuk mengubah ciphertext menjadi plaintext, disebut dekripsi(decryption). Menurut ISO 7498-2, terminologi yang lebih tepat untuk

proses ini adalah “decipher”. Cryptanalysis adalah seni dan ilmu untuk memecahkan ciphertext tanpa bantuan kunci. Cryptanalystadalah pelaku atau praktisi yang menjalankan cryptanalysis. Cryptology merupakan gabungan dari cryptography dan cryptanalysis.

Enkripsi

Enkripsi digunakan untuk menyandikan data-data atauinformasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (encrypted) dengan menggunakan sebuah kunci (key). Untuk membuka (decrypt) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus private key cryptography) atau dengan kunci yang berbeda (untuk kasus public key cryptography).

EVALUASI KEAMANAN SISTEM INFORMASI

Apabila anda telah memiliki sebuah sistem informasi, bab ini akan membantu anda untuk mengevaluasi keamanan sistem informasi yang anda miliki.

Meski sebuah sistem informasi sudah dirancang memiliki perangkat pengamanan, dalam operasi masalah keamanan harus selalu dimonitor. Hal ini disebabkan oleh beberapa hal, antara lain:

- Ditemukannya lubang keamanan (security hole) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.
- Kesalahan konfigurasi. Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.

- Penambahan perangkat baru (hardware dan/atau software) yang menyebabkan menurunnya tingkat security atau berubahnya metoda untuk mengoperasikan sistem. Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

MENGAMANKAN SISTEM INFORMASI

Pada umunya, pengamanan dapat dikategorikan menjadi dua jenis : pencegahan (preventif) dan pengobatan (recovery). Usaha pencegahan dilakukan agar sistem informasi tidak memiliki lubang keamanan, sementara usaha-usaha pengobatan dilakukan apabila lubang keamanan sudah dieksploitasi.

Pengamanan sistem informasi dapat dilakukan melaluibeberapa layer yang berbeda. Misalnya di layer "transport", dapat digunakan "Secure Socket Layer" (SSL). Metoda ini umum digunakan untuk server web. Secara fisik, sistem anda dapat juga diamankan dengan menggunakan "firewall" yang memisahkan sistem anda dengan Internet. Penggunaan teknik enkripsi dapat dilakukan di tingkat aplikasi sehingga data-data anda atau e-mail anda tidak dapat dibaca oleh orang yang tidak berhak.

Mengatur akses (Access Control)

Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme "authentication" dan "access control". Implementasi dari mekanisme ini antara lain dengan menggunakan "password".

Di sistem UNIX dan Windows NT, untuk menggunakan sebuah sistem atau komputer, pemakai diharuskan melalui proses authentication dengan menuliskan "userid" dan "password". Informasi yang diberikan ini dibandingkan dengan userid dan password yang beradadi sistem. Apabila keduanya valid, pemakai yang

bersangkutan diperbolehkan menggunakan sistem. Apabila ada yang salah, pemakai tidak dapatmenggunakan sistem. Informasi tentang kesalahan ini biasanya dicatat dalam berkas log . Besarnya informasi yang dicatat bergantung kepada konfigurasi dari system setempat. Misalnya, ada yang menuliskan informasi apabila pemakai memasukkan useriddan passwordyang salah sebanyak tiga kali. Ada juga yang langsung menuliskan informasi ke dalam berkas log meskipun baru satu kali salah. Informasi tentang waktu kejadian juga dicatat. Selain itu asal hubungan (connection) juga dicatat sehingga administrator dapat memeriksa keabsahan hubungan.

Setelah proses authentication, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah access control. Access controlini biasanya dilakukan dengan mengelompokkan pemakai dalam "group". Ada group yang berstatus pemakai biasa, ada tamu, dan ada juga administrator atau super user yang memiliki kemampuan lebih dari group lainnya. Pengelompokan ini disesuaikan dengan kebutuhan dari penggunaan sistem anda. Di lingkungan kampus mungkin ada kelompok mahasiswa, staf, karyawan, dan administrator. Sementara itu di lingkungan bisnis mungkin ada kelompok finance, engineer , marketing, dan seterusnya.

KELEBIHAN MENGGUNAKAN SISTEM KEAMAN INFORMASI BERBASIS WEB BASE

- Karena beroperasi di halaman situs web, maka fungsi e-mail dapat diakses dari berbagai tempat sepanjang dapat terkoneksi dengan internet.
- Tidak memerlukan mail client karena dapat berinteraksi dengan layanan tersebut langsung dari situs web.

KEKURANGAN MENGGUNAKAN SISTEM KEAMAN INFORMASI BERBASIS WEB BASE

- Pada saat mengakses akun e-mail, koneksi tidak boleh terputus.
- E-mail sulit diarsipkan, karena tersimpan di server penyedia layanan e-mail.
- Jika server mengalami masalah, ada kemungkinan e-mail dan bahkan akun e-mail dapat hilang begitu saja.