Bab 26

Kendala Penggunaan Kriptografi

Penggunaan kriptografi memang tidak dapat dihindarkan, dan kemajuan dalam ilmu dan teknologi kriptografi telah membuat penggunaan kriptografi cukup mudah untuk berbagai aplikasi. Namun masih ada beberapa kendala yang menghambat penggunaan kriptografi secara lebih luas. Kita akan bahas beberapa diantaranya di bab ini.

26.1 Manajemen Kunci

Manajemen kunci jelas merupakan sesuatu yang penting dalam penggunaan kriptografi. Komputerisasi manajemen kunci biasanya dilakukan menggunakan *public key infrastructure*. Di bab 23 telah kita bahas dua pendekatan yang berbeda untuk *public key infrastructure*:

- pendekatan PGP, dan
- pendekatan X.509.

Pendekatan PGP cocok untuk komunitas terbuka, namun tidak dapat digunakan dalam skala besar. Sebaliknya, pendekatan X.509 dapat digunakan dalam skala besar, namun tidak cocok untuk komunitas terbuka. Sampai saat ini belum ada pendekatan *public key infrastructure* yang efektif untuk penggunaan skala besar dalam komunitas terbuka.

Pada tingkat manajemen kunci yang lebih rinci, juga terdapat beberapa kendala, antara lain dalam hal:

- penyimpanan kunci privat oleh pengguna, dan

- manajemen *certificate*.

Dalam hal penyimpanan kunci privat oleh pengguna, ada solusi yang cukup baik jika ongkos bukan merupakan penghambat, yaitu solusi perangkat seperti *crypto device*. Akan tetapi, untuk penggunaan lebih luas, solusi perangkat masih terlalu mahal. Solusi murah dan populer saat ini adalah dengan *password protection* dimana kunci biasanya disimpan dalam *file*. Namun solusi ini rentan terhadap masalah *password*, diantaranya:

- *password* dapat terlupakan,
- *password* lebih mudah untuk dicuri dibandingkan perangkat, dan
- banyak *password* yang mudah untuk diterka.

Dalam hal manajemen *certificate*, hal yang dapat menjadi kendala penggunaan secara efektif adalah sulitnya untuk menentukan apakah suatu *certificate* masih *valid*. Untuk keperluan tertentu seperti identitas *web site*, ini mungkin bukan masalah besar. Akan tetapi untuk suatu komunitas dimana nilai suatu transaksi bisa sangat besar, ini menjadi masalah penting. Di bagian 23.2, kita telah bahas bagaimana konsep *certificate revocation* tidak efektif untuk keperluan ini. Mekanisme yang lebih baik daripada *certificate revocation* diperlukan untuk manajemen validitas *certificate*.

26.2 Sistem Terlalu Rumit

Yang dimaksud dengan sistem terlalu rumit disini adalah secara konseptual. Jika sistem terlalu rumit secara konseptual, maka sulit bagi pengguna untuk memahami cara kerja sistem. Akibat dari ketidak-pahaman atau kesalah-pahaman pengguna terhadap cara kerja sistem bisa jadi:

- sistem tidak digunakan dengan benar, atau
- sistem tidak digunakan.

Sebagai contoh, cara kerja suatu *public key infrastructure* tidak dipahami oleh sebagian pengguna karena terlalu rumit. Kesalah-pahaman dapat diperparah oleh antarmuka yang terlalu menyederhanakan, misalnya dalam penggunaan *certificate* untuk *secure web browsing*. Akibatnya, sistem bisa digunakan dengan tidak benar, misalnya menganggap bahwa transaksi dengan *web site* yang mempunyai *certificate* dianggap aman, padahal *certificate* hanya memberi jaminan identitas *web site*, tidak memberi jaminan bahwa pemilik *web site* dapat dipercaya. Pengguna yang tidak paham dengan cara kerja *public key infrastructure* dapat juga menghindar dari penggunaannya, misalnya dengan tidak

mengenkripsi *email* yang sensitif. Ini jelas berbahaya karena *email* dapat disadap, dan merupakan contoh dimana pengguna melakukan hal yang tidak aman karena merasa terlalu sulit untuk melakukan hal yang aman.

Standard aplikasi kriptografi kadang juga menggunakan konsep yang terlalu rumit. Misalnya konsep *distinguished name* dalam *certificate* berbasis X.509. Ini diperparah dengan adanya berbagai *profile* (istilah yang digunakan untuk lokalisasi standard) yang dibuat oleh berbagai negara dan organisasi. Akibatnya, berbagai program memproses *certificate* secara berbeda, *inter-operability* menjadi korban: *certificate* yang dibuat menggunakan suatu program dapat ditolak oleh program lain karena dianggap tidak memiliki format yang benar, padahal kedua program mengimplementasi standard X.509.

Rumitnya cara kerja suatu sistem secara konseptual kadang diperparah oleh implementasi yang menambah kerumitan. Sebagai contoh, antarmuka yang tidak intuitif dan tidak sesuai dengan cara kerja secara konseptual, dapat mempersulit penggunaan sistem. Antarmuka suatu sistem harus dibuat sesederhana mungkin, tanpa terlalu menyederhanakan, dan sesuai dengan cara kerja sistem secara konseptual.

26.3 Sistem Tidak Sesuai Kebutuhan

Banyak sistem yang tidak sesuai kebutuhan, contohnya sistem e-commerce yang mengandalkan *certificate authority* untuk pengamanan. Padahal yang diperlukan oleh kedua belah pihak adalah suatu *approval* oleh entitas yang dapat memberi jaminan bahwa transaksi bebas dari penipuan.

Solusi yang diberikan oleh *vendor* kerap tidak sesuai dengan kebutuhan *client*. Ini bisa terjadi karena:

- *vendor* tidak memahami kebutuhan *client*, atau
- *vendor* lebih mementingkan penjualan solusi daripada kebutuhan *client*.

Ketidak-pahaman *vendor* terhadap kebutuhan *client* biasanya terjadi karena masalah komunikasi. *Vendor* cenderung melihat dari sisi teknologi, sedangkan *client* kerap tidak paham dengan teknologi. Kerap *client* juga tidak tahu atau tidak bisa menjelaskan apa yang dibutuhkan. Terlalu sering proses *requirements analysis* diremehkan kedua belah pihak padahal proses itu sangat penting. Proses mencari tahu kebutuhan dan kemauan *client* sebaiknya merupakan proses yang cukup panjang dimana:

1. *Client* mengungkapkan keinginannya mengenai sistem.
2. *Vendor* mempelajari keinginan *client* lalu membuat *prototype* atau/dan *mockup* sistem sebagai rencana solusi.

3. *Vendor* memberi demonstrasi *prototype* atau/dan *mockup*.
4. *Client* memberi *feedback* berdasarkan demonstrasi.
5. *Vendor* merevisi *prototype* atau/dan *mockup* berdasarkan *feedback* dari *client*.

Langkah 3 sampai dengan 5 dapat diulang beberapa kali hingga *client* dan *vendor* cukup puas dengan rencana solusi.

Masalah *vendor* lebih mementingkan penjualan solusi daripada kebutuhan *client* dapat diatasi jika *client* tidak terlalu gampang terpengaruh oleh *sales pitch* dari *vendor* dan cukup mengetahui esensi dari kebutuhannya.

26.4 Ringkasan

Meskipun kemajuan dalam ilmu dan teknologi kriptografi telah membuat penggunaan kriptografi cukup mudah untuk berbagai aplikasi, masih terdapat beberapa kendala yang menghambat penggunaan kriptografi yang lebih luas. Di bab ini telah dibahas beberapa kendala penggunaan kriptografi, termasuk masalah manajemen kunci, sistem yang terlalu rumit dan sistem yang tidak sesuai dengan kebutuhan.