Pertemuan 11
Security System Terdistribusi

Pokok Bahasan

- Konsep security
- Kesederhanaan
- Cryptography

Konsep Security

Deskripsi keamanan dalam sistem terdistribusi dengan memperhatikan beberapa masalah keamanan umum. Pertama, perlu untuk mendefinisikan apa itu sistem yang aman. Dalam hal ini dibedakan kebijakan keamanan dari mekanisme keamanan. dan lihatlah sistem area luas (Global) yang mana kebijakan keamanannya telah dirumuskan secara eksplisit. Perhatian kedua adalah mempertimbangkan beberapa masalah desain umum untuk sistem yang aman.

Keamanan dalam sistem komputer sangat terkait dengan gagasan ketergantungan. Secara informal, sistem komputer yang dapat diandalkan adalah sistem yang dapat dipercaya untuk memberikan. Namun, jika ingin menaruh kepercayaan pada sistem komputer, maka kerahasiaan dan integritas juga harus diperhitungkan. Kerahasiaan mengacu pada properti sistem komputer di mana informasinya hanya diungkapkan kepada pihak yang berwenang.

Integritas adalah karakteristik bahwa perubahan pada aset sistem hanya dapat dilakukan dengan cara yang disahkan. Dengan kata lain, perubahan yang tidak tepat dalam sistem komputer yang aman harus dapat dideteksi dan dipulihkan. Aset utama dari setiap sistem komputer adalah perangkat keras, perangkat lunak, dan datanya.

Cara lain untuk melihat keamanan dalam sistem komputer adalah bahwa diupayakan melindungi layanan dan data yang ditawarkannya terhadap ancaman keamanan. Ada empat jenis ancaman keamanan untuk dipertimbangkan:

1. Intersepsi
2. Interupsi
3. Modifikasi
4. Fabrikasi

Konsep intersepsi merujuk pada situasi di mana pihak yang tidak berwenang telah memperoleh akses ke layanan atau data. Contoh khas intersepsi adalah di mana komunikasi antara dua pihak telah didengar oleh orang lain. Intersepsi juga terjadi ketika data disalin secara ilegal, misalnya, setelah membobol direktori pribadi seseorang dalam sistem file.

Contoh interupsi misalnya, ketika file rusak atau hilang. Gangguan yang lebih umum mengacu pada situasi di mana layanan atau data menjadi tidak tersedia, tidak dapat digunakan, dihancurkan, dan sebagainya. Dalam hal ini, penolakan serangan layanan di mana seseorang dengan jahat berusaha membuat layanan tidak dapat diakses oleh pihak lain adalah ancaman keamanan yang digolongkan sebagai ganggu

Modifikasi melibatkan perubahan data yang tidak sah atau perusakan dengan layanan sehingga tidak lagi mematuhi spesifikasi aslinya. Contoh modifikasi termasuk memotong dan kemudian mengubah data yang dikirimkan, merusak entri basis data, dan mengubah program sehingga secara diam-diam mencatat aktivitas penggunanya.

Fabrikasi mengacu pada situasi di mana data atau aktivitas tambahan dihasilkan yang biasanya tidak ada. Misalnya, penyusup dapat mencoba untuk menambahkan entri ke dalam file kata sandi atau basis data. Demikian juga, kadang-kadang mungkin untuk masuk ke sistem dengan memutar ulang pesan yang dikirim sebelumnya. Dengan menemukan contoh-contoh seperti itu nanti dalam pembahasan ini. Perhatikan bahwa interupsi, modifikasi, dan fabrikasi masing-masing dapat dilihat sebagai bentuk pemalsuan data.

Cukup dengan menyatakan bahwa suatu sistem harus dapat melindungi dirinya dari semua ancaman keamanan yang mungkin terjadi bukanlah cara untuk benar-benar membangun sistem yang aman. Yang pertama dibutuhkan adalah deskripsi persyaratan keamanan, yaitu kebijakan keamanan. Kebijakan keamanan menjelaskan dengan tepat tindakan apa yang diizinkan oleh entitas dalam suatu sistem dan mana yang dilarang. Entitas meliputi pengguna, layanan, data, mesin, dan sebagainya. Begitu kebijakan keamanan telah ditetapkan, menjadi mungkin untuk berkonsentrasi pada mekanisme keamanan yang dengannya suatu kebijakan dapat ditegakkan. Mekanisme keamanan penting adalah: 1. Enkripsi 2. Otentikasi 3. Otorisasi 4. Audit

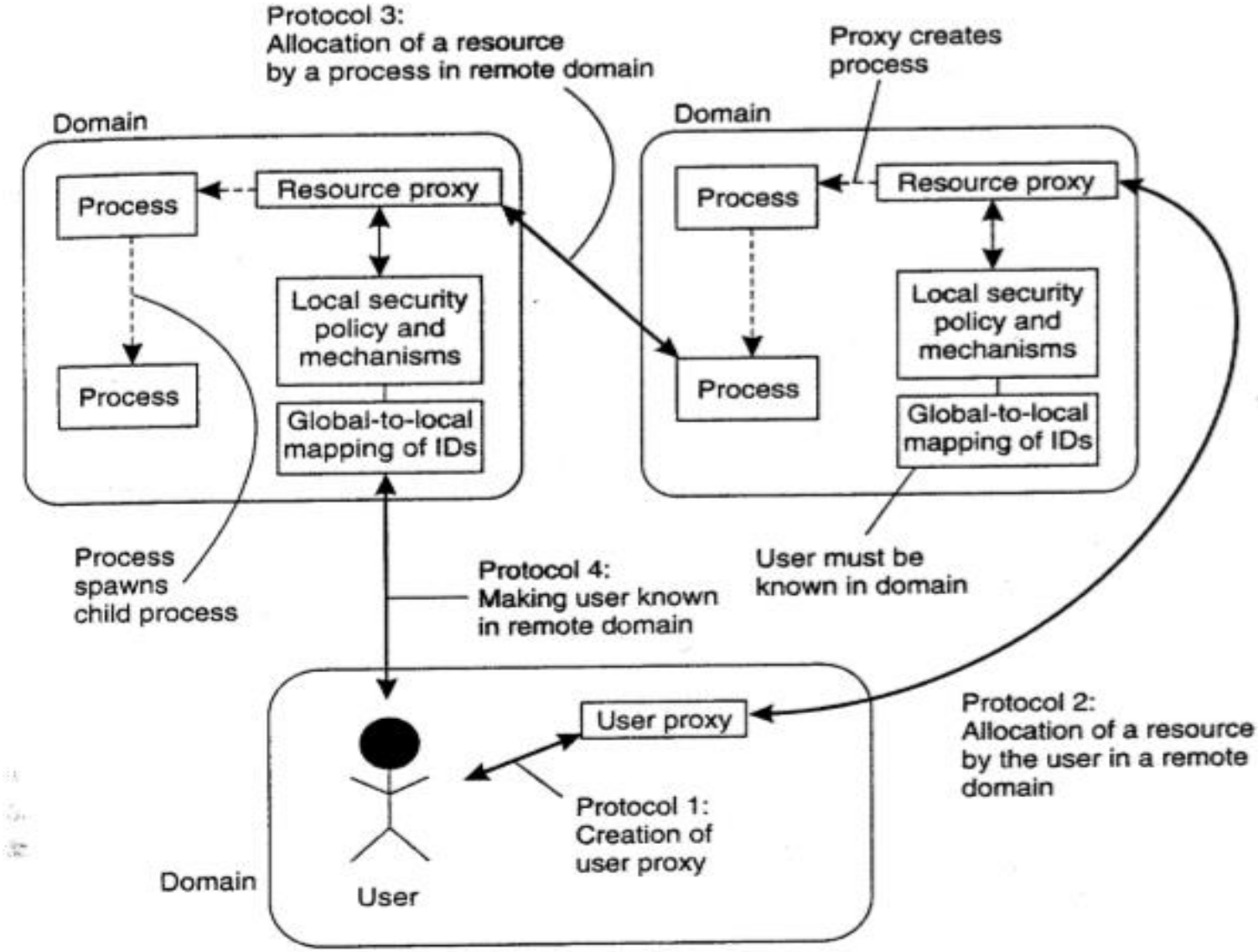
Enkripsi sangat penting untuk keamanan komputer. Enkripsi mengubah data menjadi sesuatu yang tidak dapat dipahami oleh penyerang. Dengan kata lain, enkripsi menyediakan sarana untuk mengimplementasikan kerahasiaan data. Selain itu, enkripsi memungkinkan untuk memeriksa apakah data telah dimodifikasi. Dengan demikian juga memberikan dukungan untuk pemeriksaan integritas.

Otentikasi digunakan untuk memverifikasi identitas yang diklaim pengguna, klien, server, host, atau entitas lainnya. Dalam kasus klien, premis dasarnya adalah bahwa sebelum layanan mulai melakukan pekerjaan apa pun atas nama klien, layanan harus mempelajari identitas klien (kecuali layanan tersedia untuk semua). Biasanya, pengguna diautentikasi dengan kata sandi, tetapi ada banyak cara lain untuk mengautentikasi klien. Setelah klien diautentikasi, perlu untuk memeriksa apakah klien itu berwenang untuk melakukan tindakan yang diminta. Akses ke catatan dalam database medis adalah contoh khas. Bergantung pada siapa yang mengakses database. izin dapat diberikan untuk membaca catatan, untuk memodifikasi bidang tertentu dalam catatan, atau untuk menambah atau menghapus catatan.

Arsitektur keamanan Global pada dasarnya terdiri dari entitas seperti pengguna, proxy pengguna, proxy sumber daya, dan proses umum. Entitas-entitas ini terletak di domain dan berinteraksi satu sama lain. Secara khusus, arsitektur keamanan mendefinisikan empat protokol yang berbeda, seperti yang diilustrasikan pada Gambar. Protokol pertama menjelaskan dengan tepat bagaimana pengguna dapat membuat proxy pengguna dan mendelegasikan hak untuk proxy itu. Secara khusus, untuk membiarkan proxy pengguna bertindak atas nama penggunanya, pengguna memberikan proxy seperangkat kredensial yang sesuai.

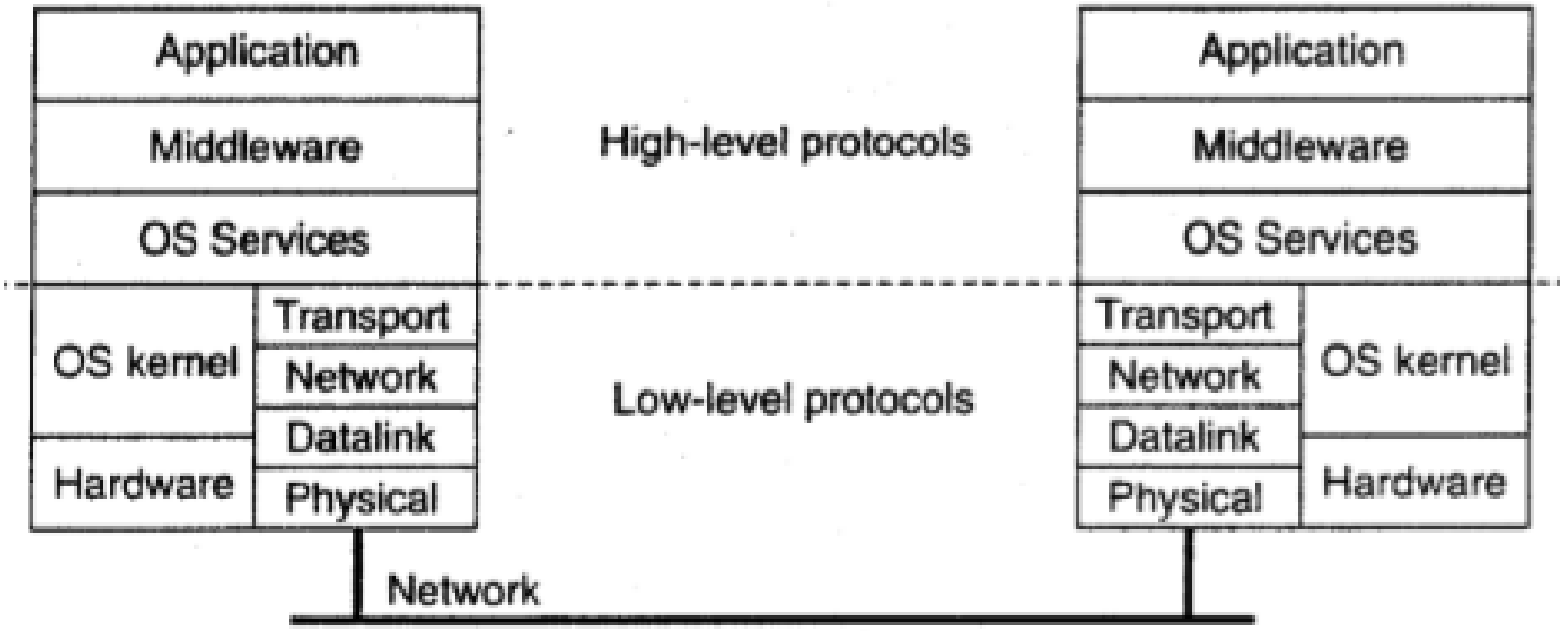
Protokol kedua menentukan bagaimana proxy pengguna dapat meminta alokasi sumber daya di domain jauh. Intinya, protokol memberi tahu proxy sumber daya untuk membuat proses di domain jauh setelah otentikasi bersama telah terjadi. Proses itu mewakili pengguna (seperti halnya proxy pengguna), tetapi beroperasi dalam domain yang sama dengan sumber daya yang diminta. Proses ini diberikan akses ke sumber daya tunduk pada keputusan kontrol akses lokal ke domain itu.

Proses yang dibuat dalam domain jarak jauh dapat memulai perhitungan tambahan di domain lain. Akibatnya, sebuah protokol diperlukan untuk mengalokasikan sumber daya di domain jauh seperti yang diminta oleh proses selain proxy pengguna. Dalam sistem Globus, jenis alokasi ini dilakukan melalui proxy pengguna, dengan membiarkan suatu proses memilikinya proxy pengguna terkait meminta alokasi sumber daya, intinya mengikuti protokol kedua.



Gambar 1. Global Security Architectur

Masalah penting dalam merancang sistem yang aman adalah memutuskan di tingkat mana mekanisme keamanan harus ditempatkan. Level dalam konteks ini terkait dengan organisasi logis dari suatu sistem menjadi sejumlah lapisan. Sebagai contoh, jaringan komputer sering disusun menjadi beberapa lapisan mengikuti beberapa model.



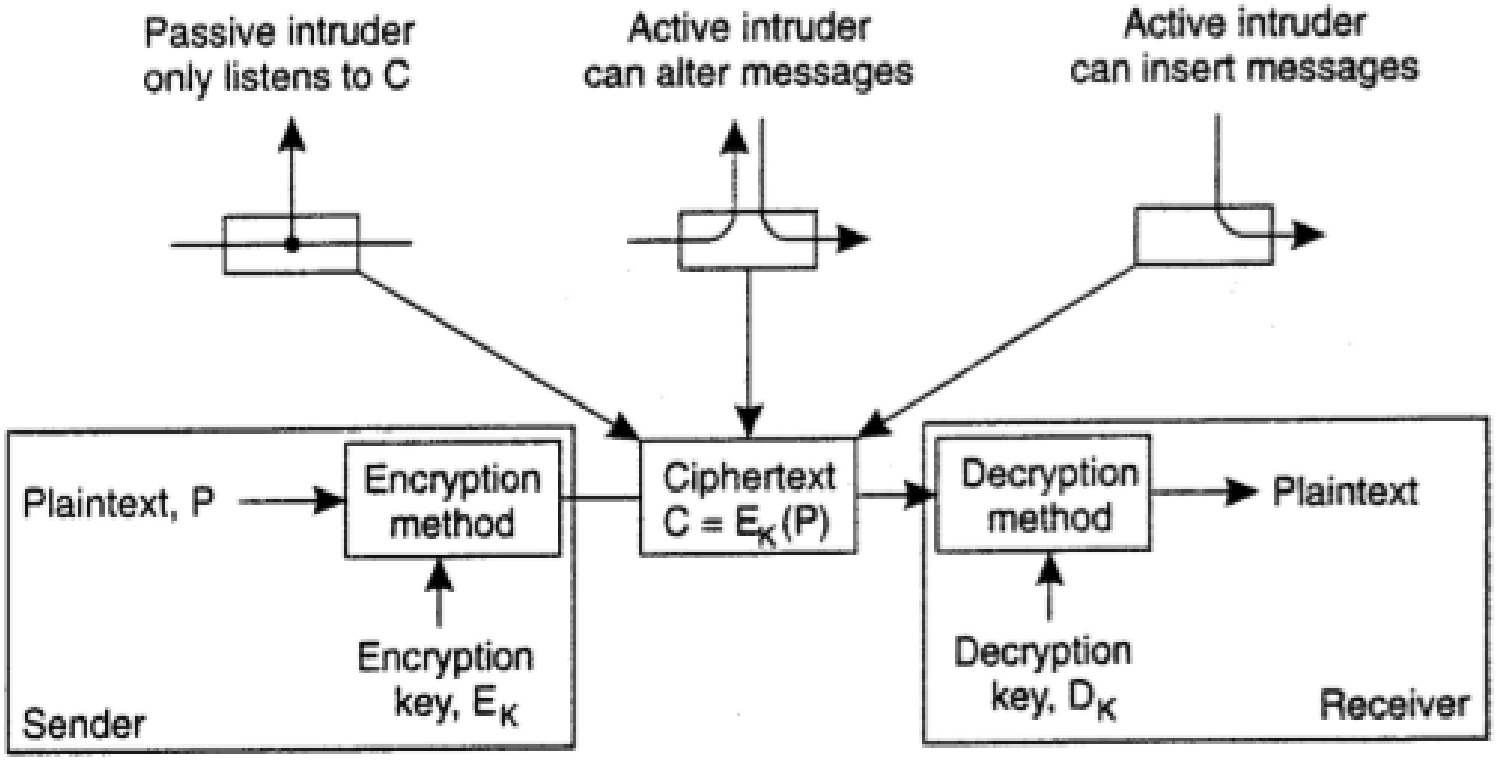
Gambar 2. Organisasi logis dari sistem terdistribusi menjadi beberapa lapisan.

Kesederhanaan (Simplicity)

Masalah desain penting lainnya yang terkait dengan memutuskan di mana lapisan untuk menempatkan mekanisme keamanan adalah kesederhanaan. Merancang sistem komputer yang aman umumnya dianggap sebagai tugas yang sulit. Akibatnya, jika seorang perancang sistem dapat menggunakan beberapa, mekanisme sederhana yang mudah dipahami dan dipercaya untuk bekerja, semakin baik itu.

Cryptography

Dasar keamanan dalam sistem terdistribusi adalah penggunaan teknik kriptografi. Ide dasar menerapkan teknik-teknik ini sederhana. Pertimbangkan pengirim S yang ingin mengirimkan pesan m ke penerima R. Untuk melindungi pesan dari ancaman keamanan, pengirim pertama-tama mengenkripsi pesan itu menjadi pesan yang tidak dapat dipahami m ', dan kemudian mengirim m' ke R. R, karena itu, harus mendekripsi menerima pesan ke dalam bentuk aslinya m. Enkripsi dan dekripsi dilakukan dengan menggunakan metode kriptografi yang diparameterisasi oleh kunci, seperti yang ditunjukkan pada Gambar.3. Bentuk asli dari pesan yang dikirim disebut plaintext, ditampilkan sebagai P pada Gambar 3; bentuk terenkripsi disebut sebagai ciphertext, diilustrasikan sebagai C.



Gambar 3. Intruders and eavesdroppers in communication

Untuk menggambarkan berbagai protokol keamanan yang digunakan dalam membangun layanan keamanan untuk sistem terdistribusi, penting untuk memiliki notasi untuk menghubungkan plaintext, ciphertext, dan kunci. Mengikuti konvensi notasi umum, akan menggunakan C = EK (P) untuk menyatakan bahwa ciphertext C diperoleh dengan mengenkripsi plaintext P menggunakan kunci K. Demikian juga, P = DK (C) digunakan untuk mengekspresikan dekripsi ciphertext C menggunakan kunci K, menghasilkan plaintext .

aat mentransfer pesan sebagai ciphertext C, ada tiga serangan berbeda yang perlu dilindungi, dan enkripsi yang membantu. Pertama, penyusup dapat mencegat pesan tanpa pengirim atau penerima menyadari bahwa menguping sedang terjadi, jika pesan yang dikirim telah dienkripsi sedemikian rupa sehingga tidak dapat dengan mudah didekripsi tanpa kunci yang tepat, intersepsi tidak berguna: penyusup hanya akan melihat data yang tidak dapat dipahami. (Ngomong-ngomong, fakta saja bahwa suatu pesan sedang dikirim mungkin terkadang cukup bagi pengganggu untuk menarik kesimpulan.

Jenis serangan kedua yang perlu ditangani adalah memodifikasi pesan. Mengubah plaintext itu mudah; memodifikasi ciphertext yang telah dienkripsi dengan benar jauh lebih sulit karena penyusup pertama-tama harus mendekripsi pesan sebelum dia dapat memodifikasinya secara bermakna. Selain itu, ia juga harus mengenkripsi lagi dengan benar atau penerima dapat melihat bahwa pesan telah dirusak.

Jenis serangan ketiga adalah ketika penyusup menyisipkan pesan terenkripsi ke dalam sistem komunikasi, berusaha membuat R percaya pesan-pesan ini berasal dari S. Lagi. seperti yang akan terlihat dalam pembahasan ini, enkripsi dapat membantu melindungi terhadap serangan semacam itu. Perhatikan bahwa jika penyusup dapat mengubah pesan, ia juga dapat menyisipkan pesan.