Ringkasan Materi:

1. Ancaman dari Mobile Code
2. Perancangan sistem yang aman
3. Kebijakan dan mekanisme
4. **Ancaman dari Mobile Code**

Mobile code adalah kode perangkat lunak yang dapat dieksekusi di beberapa perangkat atau lingkungan. Ancaman dari mobile code muncul ketika kode ini dapat diunduh dan dieksekusi di perangkat yang berbeda tanpa diketahui atau dikendalikan sepenuhnya oleh pengguna. Beberapa ancaman yang terkait dengan mobile code meliputi:

***a. Malware***: Mobile code dapat digunakan untuk menyebarkan malware seperti virus, trojan, atau ransomware ke perangkat yang tidak berjaga-jaga. Malware dapat merusak data, mencuri informasi pribadi, atau merusak sistem.

***b. Eksploitasi Keamanan***: Penjahat siber dapat memanfaatkan mobile code untuk mengeksploitasi kerentanan keamanan di perangkat yang menjalankannya. Ini dapat menyebabkan pencurian data atau kerusakan sistem.

***c. Phishing***: Penipu dapat menggunakan mobile code untuk meluncurkan serangan phishing yang mengelabui pengguna dan mencuri informasi login atau data pribadi.

***d. Penyebaran Malware dan Spam***: Mobile code dapat digunakan untuk mengirimkan spam atau memfasilitasi penyebaran malware ke perangkat lain.

1. **Perancangan Sistem yang Aman dalam Sistem Terdistribusi**

Perancangan sistem yang aman dalam sistem terdistribusi adalah proses merancang dan mengimplementasikan sistem yang menjaga keamanan data dan operasi dalam lingkungan yang terdistribusi. Beberapa langkah yang dapat diambil untuk merancang sistem yang aman yaitu:

***a. Identifikasi Ancaman***: Identifikasi potensi ancaman keamanan yang dapat terjadi dalam lingkungan terdistribusi, seperti serangan jaringan, penipuan, atau pencurian data.

***b. Penggunaan Enkripsi***: Menggunakan enkripsi untuk melindungi data saat berpindah melalui jaringan atau disimpan di tempat penyimpanan terdistribusi.

***c. Otentikasi dan Otorisasi***: Memastikan bahwa hanya pengguna yang sah memiliki akses yang sesuai ke sistem dan data dengan mengimplementasikan otentikasi yang kuat dan mekanisme otorisasi.

***d. Audit dan Monitoring***: Melakukan pemantauan dan audit terus-menerus terhadap sistem untuk mendeteksi aktivitas mencurigakan dan melacak kejadian yang tidak sah.

***e. Pemulihan dan Cadangan***: Merencanakan strategi pemulihan darurat dan cadangan data untuk menghadapi insiden keamanan.

***f. Pembaruan Perangkat Lunak***: Mengatur pembaruan perangkat lunak secara berkala untuk mengatasi kerentanan keamanan yang baru ditemukan.

1. **Kebijakan dan Mekanisme dalam Sistem Terdistribusi**

Kebijakan keamanan dan mekanisme dalam sistem terdistribusi mengacu pada pedoman dan prosedur yang ditetapkan untuk melindungi sistem dan data dalam lingkungan yang terdistribusi. Beberapa elemen yang terlibat dalam hal ini adalah:

***a. Kebijakan Keamanan***: Menetapkan aturan dan pedoman yang mengatur akses, penggunaan, dan perlindungan data dalam sistem terdistribusi.

***b. Mekanisme Otorisasi***: Menerapkan kontrol akses yang ketat untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sumber daya sistem.

***c. Mekanisme Enkripsi***: Menggunakan teknik enkripsi untuk melindungi data saat berpindah melalui jaringan atau disimpan di server terdistribusi.

***d. Pemantauan dan Pembaruan***: Menerapkan mekanisme pemantauan yang kontinu dan pembaruan sistem untuk menjaga keamanan sistem terdistribusi.

***e. Pelatihan Pengguna***: Melakukan pelatihan pengguna untuk memastikan bahwa mereka memahami kebijakan keamanan dan dapat berkontribusi pada keamanan sistem.

***f. Manajemen Kejadian Keamanan***: Menerapkan prosedur untuk menangani insiden keamanan dan merespons serangan atau ancaman dengan cepat dan efektif.

Semua tiga elemen ini penting untuk membangun dan menjaga sistem terdistribusi yang aman. Keamanan harus dipandang sebagai prioritas dalam pengembangan dan operasi sistem terdistribusi.