Cloud Security

Keamanan komputer di milenium baru

- Dalam dunia yang saling terhubung, berbagai perwujudan malware dapat bermigrasi dengan mudah dari satu sistem ke sistem lainnya, melintasi batas negara dan menginfeksi sistem di seluruh dunia.
- Keamanan sistem komputasi dan komunikasi mengambil urgensi baru karena masyarakat menjadi semakin bergantung pada infrastruktur informasi. Bahkan infrastruktur kritis suatu negara dapat diserang dengan memanfaatkan kelemahan dalam keamanan komputer.
- Baru-baru ini, istilah cyberwarfare telah memasuki kamus yang berarti "tindakan oleh negara-bangsa untuk menembus komputer atau jaringan negara lain untuk tujuan menyebabkan kerusakan atau gangguan"

Cloud security

- Cloud computing adalah lingkungan yang kaya akan target untuk individu jahat dan organisasi kriminal.
- Perhatian utama bagi pengguna yang sudah ada dan bagi calon pengguna baru layanan komputasi awan. Mengalihdayakan komputasi ke cloud menghasilkan masalah keamanan dan privasi baru.
- Standar, peraturan, dan undang-undang yang mengatur aktivitas organisasi yang mendukung komputasi awan belum diadopsi. Banyak masalah yang terkait dengan privasi, keamanan, dan kepercayaan pada komputasi awan masih jauh dari penyelesaian.
- Ada kebutuhan akan peraturan internasional yang diadopsi oleh negara-negara di mana pusat data penyedia cloud computing berada.
- Perjanjian Tingkat Layanan (Service Level Agreements (SLA)) tidak memberikan perlindungan hukum yang memadai bagi pengguna komputer cloud, sering kali dibiarkan untuk menangani peristiwa di luar kendali mereka.

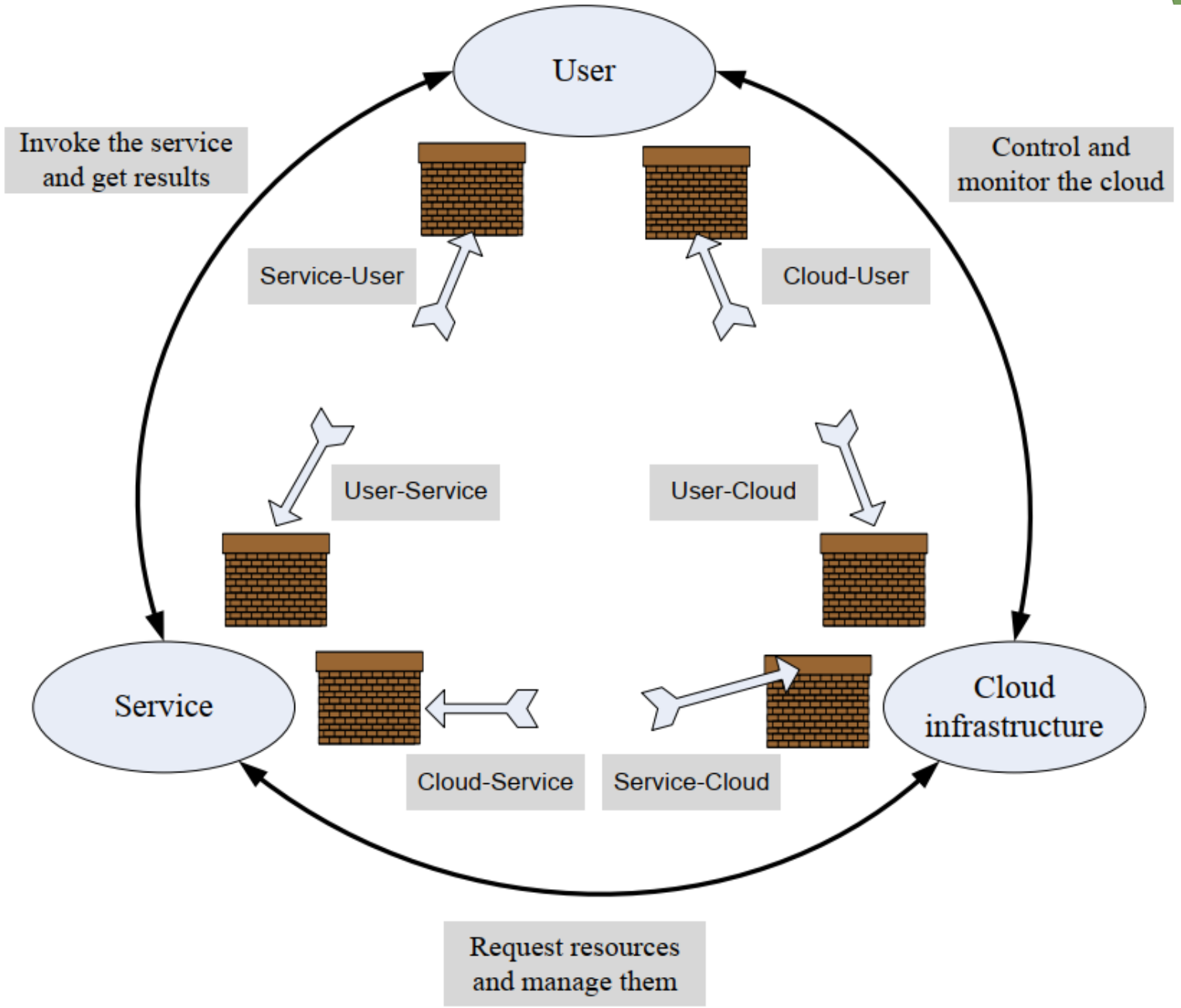
Risiko keamanan cloud

- Ancaman tradisional (Traditional threats) → dampak diperkuat karena banyaknya sumber daya cloud dan populasi pengguna yang besar yang dapat terpengaruh. Batas tanggung jawab yang kabur antara penyedia layanan cloud dan pengguna dan kesulitan untuk mengidentifikasi penyebabnya secara akurat.
- Ancaman baru (New threats) → server cloud menghosting banyak VM; beberapa aplikasi dapat berjalan di bawah setiap VM. Kerentanan multi-tenancy dan VMM membuka saluran serangan baru untuk pengguna jahat. Mengidentifikasi jalur yang diikuti oleh penyerang lebih sulit di lingkungan cloud.
- Otentikasi dan otorisasi prosedur → yang berlaku untuk satu individu tidak mencakup perusahaan.
- Kontrol pihak ketiga → menimbulkan spektrum kekhawatiran yang disebabkan oleh kurangnya transparansi dan kontrol pengguna yang terbatas.
- Ketersediaan layanan cloud → kegagalan sistem, pemadaman listrik, dan peristiwa bencana lainnya dapat mematikan layanan untuk waktu yang lama.

Serangan di lingkungan cloud computing

Tiga aktor yang terlibat; enam jenis serangan mungkin.

- Pengguna dapat diserang oleh:
  1. Layanan spoofing → sertifikat SSL, serangan pada cache browser, atau serangan phishing.
  2. Infrastruktur cloud → serangan yang berasal dari cloud atau spoof yang berasal dari infrastruktur cloud.
- Layanan dapat diserang oleh:
  3. Pengguna → Buffer overflow, injeksi SQL, dan eskalasi hak istimewa adalah jenis serangan yang umum.
  4. Infrastruktur cloud → serangan paling serius. Membatasi akses ke sumber daya, serangan terkait hak istimewa, distorsi data,menyuntikkan operasi tambahan.
- Infrastruktur cloud dapat diserang oleh:
  5. Pengguna → menargetkan sistem kontrol cloud.
  6. Layanan → meminta jumlah sumber daya yang berlebihan dan menyebabkan kehabisan sumber daya.


User
Invoke the service and get results
Control and monitor the cloud
Service-User
Cloud-User
User-Service
User-Cloud
Service
Cloud infrastructure
Cloud-Service
Service-Cloud
Request resources and manage them

Ancaman teratas terhadap cloud computing

Diidentifikasi oleh laporan Cloud Security Alliance (CSA) 2010:

- Penyalahgunaan cloud - kemampuan untuk melakukan aktivitas jahat dari cloud.
- API yang tidak sepenuhnya aman - mungkin tidak melindungi pengguna selama rentang aktivitas yang dimulai dengan autentikasi dan kontrol akses hingga pemantauan dan kontrol aplikasi selama waktu proses.
- Orang dalam yang jahat - penyedia layanan cloud tidak mengungkapkan standar dan kebijakan perekrutan mereka, jadi ini bisa menjadi ancaman serius.
- Teknologi bersama.
- Pembajakan akun.
- Kehilangan atau kebocoran data - jika satu-satunya salinan data disimpan di cloud, maka data sensitif akan hilang secara permanen saat replikasi data cloud gagal diikuti dengan kegagalan media penyimpanan.
- Profil risiko tidak diketahui - paparan ketidaktahuan atau meremehkan risiko komputasi awan.

Auditabilitas aktivitas cloud

- Kurangnya transparansi membuat kemampuan audit menjadi proposisi yang sangat sulit untuk komputasi awan.
- Pedoman audit yang diuraikan oleh National Institute of Standards (NIST) wajib bagi lembaga Pemerintah AS:
  - the Federal Information Processing Standard (FIPS).
  - the Federal Information Security Management Act (FISMA).

Keamanan - perhatian utama bagi pengguna cloud

- Akses tidak sah ke informasi rahasia dan pencurian data teratas dalam daftar kekhawatiran pengguna.
  - Data lebih rentan dalam penyimpanan, karena disimpan dalam penyimpanan untuk waktu yang lama.
  - Ancaman selama pemrosesan tidak dapat diabaikan; ancaman tersebut dapat berasal dari kelemahan dalam VMM, VM nakal, atau VMBR.
- Ada risiko akses tidak sah dan pencurian data yang ditimbulkan olehkaryawan nakal dari Penyedia Layanan Cloud (Cloud Service Provider (CSP)).
- Kurangnya standarisasi juga menjadi perhatian utama.
- Pengguna khawatir tentang penegakan hukum untuk keamanan cloud computing.
- Multi-tenancy adalah akar penyebab banyak masalah pengguna. Namun demikian, multi-tenancy memungkinkan pemanfaatan server yang lebih tinggi, sehingga biaya lebih rendah.
- Ancaman yang disebabkan oleh multi-tenancy berbeda dari satu model pengiriman cloud ke model lainnya.

Perlindungan hukum pengguna cloud

Kontrak antara pengguna dan Penyedia Layanan Cloud (CSP)harus menjelaskan secara eksplisit:

- Kewajiban CSP untuk menangani informasi sensitif yang aman dan kewajibannya untuk mematuhi undang-undang privasi.
- Kewajiban CSP atas kesalahan penanganan informasi sensitif.
- Kewajiban CSP atas kehilangan data.
- Aturan yang mengatur kepemilikan data.
- Wilayah geografis tempat informasi dan cadangan dapat disimpan.

Privacy

- Privasi → hak individu, sekelompok individu, atau organisasi untuk menjaga informasi yang bersifat pribadi atau informasi kepemilikan agar tidak diungkapkan.
- Privasi dilindungi oleh hukum; terkadang undang-undang membatasi privasi.
- Aspek utama privasi adalah: kurangnya kontrol pengguna, potensi penggunaan sekunder yang tidak sah, dan penyediaan dinamis.
- Era digital telah menghadapkan legislator dengan tantangan signifikan terkait privasi karena ancaman baru telah muncul. Misalnya, informasi pribadi yang dibagikan secara sukarela, tetapi dicuri dari situs yang diberi akses atau disalahgunakan dapat menyebabkan pencurian identitas.
- Masalah privasi berbeda untuk ketiga model cloud.

Aturan Komisi layanan web

Situs web yang mengumpulkan informasi pengenal pribadi dari atau tentang konsumen secara online diwajibkan untuk mematuhi empat praktik informasi yang adil:

- Pemberitahuan (Notice) - memberikan pemberitahuan yang jelas dan mencolok kepada konsumen tentang praktik informasi mereka, termasuk informasi apa yang mereka kumpulkan, bagaimana mereka mengumpulkannya, bagaimana mereka menggunakannya, bagaimana mereka memberikan Pilihan, Akses, dan Keamanan kepada konsumen, apakah mereka mengungkapkan informasi yang dikumpulkan kepada orang lain entitas, dan apakah entitas lain mengumpulkan informasi melalui situs.
- Pilihan (Choice) - menawarkan pilihan kepada konsumen tentang bagaimana informasi pengenal pribadi mereka digunakan. Pilihan tersebut akan mencakup penggunaan sekunder internal (seperti pemasaran kembali ke konsumen) dan penggunaan sekunder eksternal (seperti pengungkapan data ke entitas lain).
- Akses (Access) - menawarkan kepada konsumen akses yang wajar ke informasi yang dikumpulkan situs web tentang mereka, termasuk kesempatan yang wajar untuk meninjau informasi dan memperbaiki ketidakakuratan atau menghapus informasi.
- Keamanan (Security) - mengambil langkah-langkah yang wajar untuk melindungi keamanan informasi yang mereka kumpulkan dari konsumen

Privacy Impact Assessment (PIA)

- Perlunya alat yang mampu mengidentifikasi masalah privasi dalam sistem informasi.
- Tidak ada standar internasional untuk proses seperti itu, meskipun negara dan organisasi yang berbeda memerlukan laporan PIA.
- Inti dari Alat PIA yang diusulkan didasarkan pada layanan SaaS.
  - Pengguna layanan SaaS yang menyediakan akses ke alat PIA harus mengisi kuesioner.
  - Sistem menggunakan basis pengetahuan (knowledge base(KB)) yang dibuat dan dikelola oleh pakar domain.
  - Sistem menggunakan template untuk menghasilkan pertanyaan tambahan yang diperlukan dan untuk mengisi laporan PIA.
  - Sistem pakar menyimpulkan aturan mana yang dipenuhi oleh fakta dalam database dan disediakan oleh pengguna dan menjalankan aturan dengan prioritas tertinggi.

Trust

- Trust → kepercayaan yang pasti pada karakter, kemampuan, kekuatan, atau kebenaran seseorang atau sesuatu.
- Fenomena kompleks: memungkinkan perilaku kooperatif, mempromosikan bentuk organisasi yang adaptif, mengurangi konflik yang merugikan, mengurangi biaya transaksi, mempromosikan tanggapan yang efektif terhadap krisis.
- Dua kondisi harus ada agar kepercayaan dapat berkembang.
  - Risiko → kemungkinan kerugian yang dirasakan; kepercayaan tidak diperlukan jika tidak ada risiko yang terlibat, jika ada kepastian bahwa suatu tindakan dapat berhasil.
  - Saling ketergantungan → kepentingan satu entitas tidak dapat diarsipkan tanpa ketergantungan pada entitas lain.
- Hubungan kepercayaan berjalan melalui tiga fase:
  1. Fase membangun, saat kepercayaan terbentuk.
  2. Fase stabilitas, ketika kepercayaan ada.
  3. Fase pembubaran, ketika kepercayaan menurun.
- Entitas harus bekerja sangat keras untuk membangun kepercayaan, tetapi mungkin kehilangan kepercayaan dengan sangat mudah.

Internet trust

- Mengaburkan atau sama sekali tidak memiliki dimensi karakter dan kepribadian, sifat hubungan, dan karakter institusional dari kepercayaan tradisional.
- Menawarkan individu kemampuan untuk mengaburkan atau menyembunyikan identitas mereka. Anonimitas mengurangi isyarat yang biasanya digunakan dalam penilaian kepercayaan.
- Identitas sangat penting untuk mengembangkan hubungan kepercayaan, memungkinkan kita untuk mendasarkan kepercayaan kita pada sejarah masa lalu interaksi dengan suatu entitas. Anonimitas menyebabkan ketidakpercayaan karena identitas dikaitkan dengan akuntabilitas dan tanpa adanya akuntabilitas identitas tidak dapat ditegakkan.
- Opacity memperluas identitas ke karakteristik pribadi. Mustahil untuk menyimpulkan apakah entitas atau individu yang bertransaksi dengan kita adalah yang berpura-pura, karena transaksi terjadi antara entitas yang terpisah dalam waktu dan jarak.
- Tidak ada jaminan bahwa entitas yang bertransaksi dengan kami sepenuhnya memahami peran yang mereka emban.

Bagaimana menentukan kepercayaan?

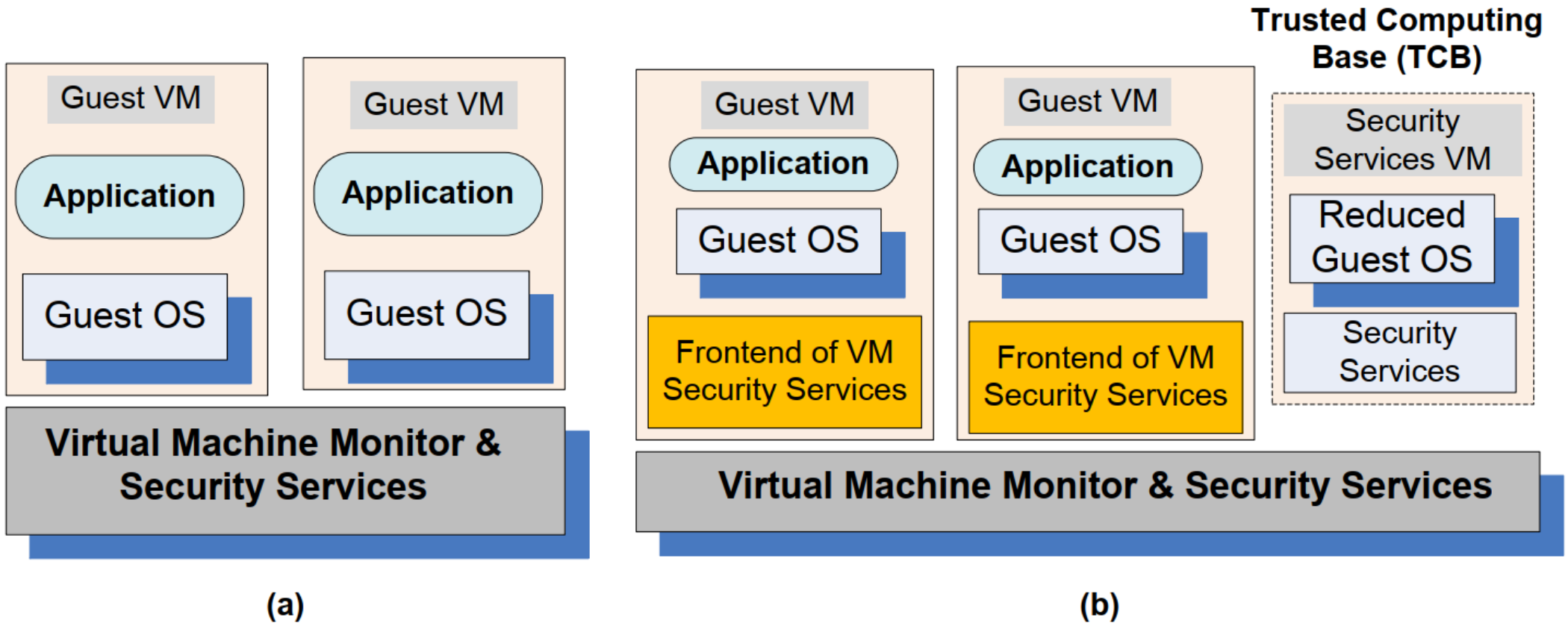
- Kebijakan dan reputasi adalah dua cara untuk menentukan kepercayaan.
  - Kebijakan mengungkapkan kondisi untuk mendapatkan kepercayaan, dan tindakan ketika beberapa kondisi terpenuhi. Kebijakan memerlukan verifikasi kredensial; kredensial dikeluarkan oleh otoritas tepercaya dan menggambarkan kualitas entitas yang menggunakan kredensial.
  - Reputasi adalah kualitas yang dikaitkan dengan entitas berdasarkan riwayat interaksi yang relatif panjang atau kemungkinan pengamatan entitas. Rekomendasi didasarkan pada keputusan kepercayaan yang dibuat oleh orang lain dan disaring melalui perspektif entitas yang menilai kepercayaan.
- Dalam konteks ilmu komputer : kepercayaan dari pihak A kepada pihak B untuk layanan X adalah keyakinan terukur dari A bahwa B berperilaku dapat diandalkan untuk periode tertentu dalam konteks tertentu (dalam kaitannya dengan layanan X).

Keamanan sistem operasi

- Sebuah fungsi penting dari sebuah OS adalah untuk melindungi aplikasi dari berbagai serangan berbahaya, misalnya, akses tidak sah ke informasi istimewa, temper dengan kode yang dapat dieksekusi, dan spoofing.
- Elemen keamanan OS wajib ada:
  - Kontrol akses→ mekanisme untuk mengontrol akses ke objek sistem.
  - Penggunaan → otentikasi mekanisme untuk mengotentikasi prinsipal.
  - Kebijakan penggunaan kriptografi → mekanisme yang digunakan untuk melindungi data
- OS Komersial tidak mendukung keamanan berlapis-lapis; hanya membedakan antara domain keamanan yang sepenuhnya memiliki hak istimewa dan domain yang sepenuhnya tidak memiliki hak istimewa.
- Mekanisme jalur tepercaya (Trusted paths) → mendukung interaksi pengguna dengan perangkat lunak tepercaya. Penting untuk keamanan sistem; jika mekanisme tersebut tidak ada, maka perangkat lunak berbahaya dapat meniru perangkat lunak tepercaya. Beberapa sistem menyediakan jalur kepercayaan untuk beberapa fungsi, seperti otentikasi login dan perubahan kata sandi, dan mengizinkan server untuk mengotentikasi klien mereka.

Keamanan mesin virtual

- VM hybrid dan host, memaparkan seluruh sistem pada kerentanan OS host.
- Dalam VM tradisional, Virtual Machine Monitor (VMM) mengontrol akses ke perangkat keras dan menyediakan isolasi VM yang lebih ketat dari satu sama lain daripada isolasi proses dalam OS tradisional.
  - VMM memiliki hak istimewa untuk mengontrol eksekusi operasi dan dapat melakukan isolasi memori serta akses disk dan jaringan.
  - VMM jauh lebih kompleks dan terstruktur lebih baik daripada sistem operasi tradisional sehingga, dalam posisi yang lebih baik untuk menanggapi serangan keamanan.
  - Tantangan utama → VMM hanya melihat data mentah mengenai status sistem operasi tamu sementara layanan keamanan biasanya beroperasi pada tingkat logis yang lebih tinggi, misalnya, pada tingkat file daripada blok disk.
- TCB Trusted Computing Base (Basis Komputasi Tepercaya) yang aman adalah kondisi yang diperlukan untuk keamanan di lingkungan mesin virtual; jika TCB terganggu maka keamanan seluruh sistem terpengaruh.



(a) Layanan keamanan virtual yang disediakan oleh VMM;
(b) VM keamanan khusus.

Ancaman berbasis VMM

- Kekurangan sumber daya dan penolakan layanan untuk beberapa VM.Kemungkinan penyebab:
  a) batas sumber daya yang dikonfigurasi dengan buruk untuk beberapa VM.
  b) VM nakal dengan kemampuan untuk melewati batas sumber daya yang ditetapkan dalam VMM.
- VM side-channel attacks : serangan berbahaya pada satu atau lebih VM oleh VM jahat di bawah VMM yang sama. Kemungkinan penyebab:
  a) kurangnya isolasi lalu lintas antar-VM yang tepat karena kesalahan konfigurasi jaringan virtual yang berada di VMM.
  b) pembatasan perangkat inspeksi paket untuk menangani lalu lintas berkecepatan tinggi, misalnya, lalu lintas video.
  c) adanya instans VM yang dibuat dari image VM yang tidak aman, misalnya image VM yang memiliki OS tamu tanpa patch terbaru.
- Serangan buffer overflow.

Ancaman berbasis VM

- Penyebaran VM nakal atau tidak aman. Pengguna yang tidak sah dapat membuat instance tidak aman dari gambar atau dapat melakukan tindakan administratif yang tidak sah pada VM yang ada. Kemungkinan penyebab:
  - konfigurasi kontrol akses yang tidak tepat pada tugas administratif VM seperti pembuatan instance, peluncuran, penangguhan, aktivasi ulang, dan sebagainya.
- Adanya image VM yang tidak aman dan rusak dalam repositori image VM. Kemungkinan penyebab:
  a) kurangnya kontrol akses ke repositori gambar VM.
  b) kurangnya mekanisme untuk memverifikasi integritas gambar, misalnya, gambar yang ditandatangani secara digital.

Keamanan virtualisasi

Status lengkap sistem operasi yang berjalan di bawah mesin virtual ditangkap oleh VM; status ini dapat disimpan dalam file dan kemudian file tersebut dapat disalin dan dibagikan. Implikasi:

- Kemampuan untuk mendukung model pengiriman IaaS. Dalam model ini pengguna memilih image yang cocok dengan lingkungan lokal yang digunakan oleh aplikasi dan kemudian mengunggah dan menjalankan aplikasi di cloud menggunakan Image ini.
- Peningkatan keandalan. Sistem operasi dengan semua aplikasi yang berjalan di bawahnya dapat direplikasi dan dialihkan ke siaga.
- Peningkatan pencegahan dan deteksi intrusi. Klon dapat mencari pola yang diketahui dalam aktivitas sistem dan mendeteksi intrusi. Operator dapat beralih ke siaga ketika peristiwa mencurigakan terdeteksi.
- Pengujian perangkat lunak yang lebih efisien dan fleksibel. Alih-alih sejumlah besar sistem khusus yang berjalan di bawah OS yang berbeda, versi yang berbeda dari setiap OS, dan patch yang berbeda untuk setiap versi, virtualisasi memungkinkan banyak instance OS untuk berbagi sejumlah kecil sistem fisik.

keuntungan dari virtualisasi

- Mekanisme langsung diterapkan dalam manajemen sumber daya kebijakan:
  - Untuk menyeimbangkan beban sistem, VMM dapat memindahkan OS dan aplikasi yang berjalan di bawahnya ke server lain ketika beban pada server saat ini sudah melebihi batas.
  - Untuk mengurangi konsumsi daya, beban server dengan beban ringan dapat dipindahkan ke server lain dan kemudian, matikan atau atur ke mode siaga server dengan beban ringan.
- Ketika logging aman dan perlindungan intrusi diterapkan pada lapisan VMM, layanan tidak dapat dinonaktifkan atau dimodifikasi. Deteksi penyusupan dapat dinonaktifkan dan logging dapat dimodifikasi oleh penyusup saat diimplementasikan pada level OS. VMM mungkin hanya dapat mencatat peristiwa yang menarik untuk analisis pasca-serangan.

Kerugian Virtualisasi

Berkurangnya kemampuan untuk mengelola sistem dan melacak statusnya.

- Jumlah sistem fisik dalam inventaris organisasi dibatasi oleh biaya, ruang, konsumsi energi, dan dukungan manusia. Membuat mesin virtual (VM) pada akhirnya mengurangi penyalinan file, oleh karena itu ledakan jumlah VM. Satu-satunya batasan untuk jumlah VM adalah jumlah ruang penyimpanan yang tersedia.
- Aspek kualitatif ledakan jumlah VM tradisional, organisasi menginstal dan memelihara versi yang sama dari perangkat lunak sistem. Dalam lingkungan virtual jumlah sistem operasi yang berbeda, versinya, dan status patch setiap versi akan sangat beragam. Heterogenitas akan membebani tim pendukung.
- Siklus hidup perangkat lunak memiliki implikasi serius pada keamanan. Asumsi tradisional siklus hidup perangkat lunak adalah garis lurus, maka manajemen patch didasarkan pada kemajuan monoton ke depan. Model eksekusi virtual memetakan ke struktur pohon daripada garis; memang, setiap saat beberapa contoh VM dapat dibuat dan kemudian, masing-masing dari mereka dapat diperbarui, patch yang berbeda diinstal, dan seterusnya.

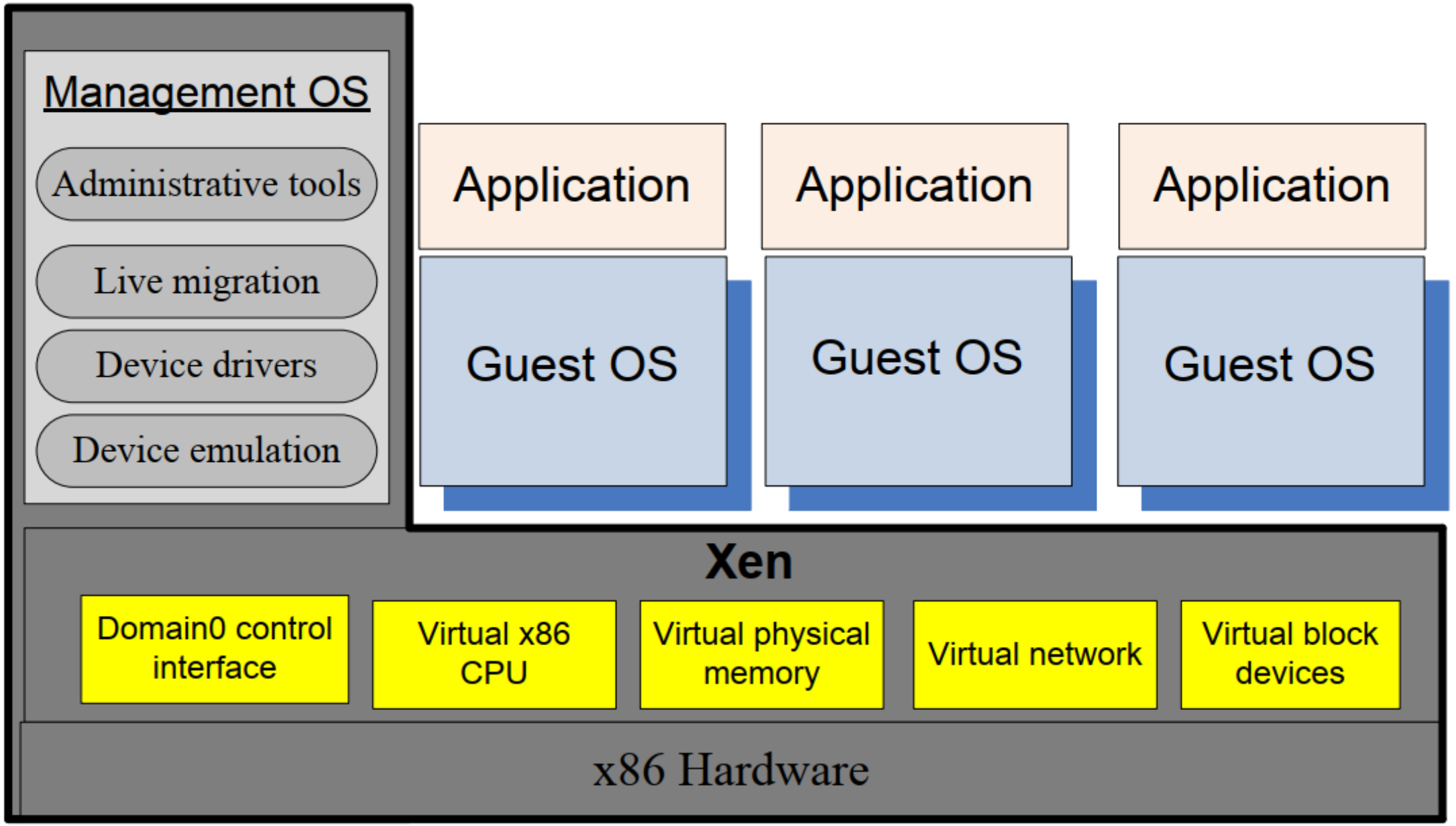
Implikasi virtualisasi pada keamanan

- Infeksi dapat berlangsung tanpa batas waktu beberapa VM yang terinfeksi mungkin tidak aktif pada saat tindakan untuk membersihkan sistem diambil dan kemudian, di lain waktu, bangun dan menginfeksi sistem lain; skenario bisa berulang.
- Dalam lingkungan komputasi tradisional, kondisi mapan dapat dicapai. Keadaan yang diinginkan ini dicapai dengan menginstal versi terbaru dari perangkat lunak sistem dan kemudian menerapkan patch terbaru ke semua sistem. Karena kurangnya kontrol, lingkungan virtual mungkin tidak akan pernah mencapai kondisi stabil seperti itu.
- Efek samping dari kemampuan untuk merekam dalam file status lengkap VM adalah kemungkinan untuk memutar kembali VM. Ini memungkinkan jenis kerentanan baru yang disebabkan oleh peristiwa yang direkam dalam memori penyerang.
- Virtualisasi merusak prinsip dasar bahwa data sensitif waktu yang disimpan pada sistem apa pun harus dikurangi seminimal mungkin.

Resiko Keamanan

Resiko keamanannya dapat berupa:

- Backdoors dan leftover credentials.
- Unsolicited connections (koneksi yang tidak diinginkan).
- Malware.


Management OS
Administrative tools
Live migration
Device drivers
Device emulation
Application
Application
Application
Guest OS
Guest OS
Guest OS
Xen
Domain0 control interface
Virtual x86 CPU
Virtual physical memory
Virtual network
Virtual block devices
x86 Hardware

Trusted Virtual Machine Monitor

Ide baru untuk monitor mesin virtual (trusted virtual machine monitor (TVMM)) tepercaya:

- Ini harus mendukung tidak hanya sistem operasi tradisional, dengan mengekspor abstraksi perangkat keras untuk platform system yang lebih luas, tetapi juga abstraksi untuk platform yang terbatas (jangan biarkan konten sistem dimanipulasi atau diperiksa oleh pemilik platform).
- Aplikasi harus diizinkan untuk membangun tumpukan perangkat lunaknya berdasarkan kebutuhannya. Aplikasi yang membutuhkan tingkat keamanan yang sangat tinggi harus berjalan di bawah OS yang terbatas yang hanya mendukung fungsionalitas yang dibutuhkan oleh aplikasi dan kemampuan untuk melakukan booting.
- Menyediakan jalur tepercaya dari pengguna ke aplikasi. Jalur seperti itu memungkinkan pengguna manusia untuk menentukan dengan pasti identitas VM yang berinteraksi dengannya dan memungkinkan VM memverifikasi identitas pengguna manusia.
- Menolak administrator untuk mendapatkan akses root.
- Dukungan pengesahan, kemampuan aplikasi yang berjalan dalam lingkup yang terbatas untuk mendapatkan kepercayaan dari pihak yang jauh, dengan mengidentifikasi dirinya sendiri secara kriptografis.

Link Video penjelasan

https://drive.google.com/file/d/1NAL4eMeJMhvS9fKdh04P1lDy5JC-KUlq/view?usp=sharing

Terimakasih