Sesi 14 **Keamanan Sistem Komputer**

Computer Security

Kuliah Online : Sistem Operasi

Dosen : Ir. Nixon Erzed MT - Tim Dosen Sistem Operasi

A. Pengantar Keamanan Sistem Komputer

Keamanan sistem komputer merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja dan proses komputer. Penerapan computer security dalam kehidupan sehari-hari berguna sebagai penjaga sumber daya sistem agar tidak digunakan, modifikasi, interupsi, dan diganggu oleh orang yang tidak berwenang. Keamanan bisa diindentifikasikan dalam masalah teknis, manajerial, legalitas, dan politis.

Computer security membahas 2 hal penting yaitu :

- Ancaman/Threats dan
- Kelemahan sistem/vulnerabillity.

Keamanan komputer memiliki 5 tujuan, yaitu:

1. Availability
2. Confidentiality
3. Data Integrity
4. Control
5. Audit

Dalam konteks sistem informasi, keamanan komputer bertujuan :

1. Perusahaan; berusaha melindungi data dan informasi dari orang yang tidak berada dalam ruang lingkupnya.
2. Ketersediaan; tujuan SIFO adalah menyediakan data dan informasi bagi mereka yang berwenang untuk menggunakannya.
3. Integritas; semua subsistem SIFO harus menyediakan gambaran akurat dari sistem fisik yang di wakilinya.

Level Sistem Keamanan

Metode pengamanan komputer dibedakan berdasarkan level keamanan, dan disusun seperti piramida, yaitu:

- Keamanan Level 0, merupakan keamanan fisik (Physical Security) atau keamanan tingkat awal. Apabila keamanan fisik sudah terjaga maka keamanan di dalam computer juga akan terjaga.

- Keamanan Level 1, terdiri dari database security, data security, dan device security. Pertama dari pembuatan database dilihat apakah menggunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan data security yaitu pendesainan database, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah device security yaitu alah yang dipakai untuk keamanan dari database tersebut.
- Keamanan Level 2, yaitu keamanan dari segi keamanan jaringan. Keamanan ini sebagai tindak lanjut dari keamanan level 1.
- Keamanan Level 3, merupakan information security. Informasi – informasi seperti kata sandi yang dikirimkan kepada teman atau file – file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut.
- Keamanan Level 4, keamanan ini adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila ada satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi.

Metoda Pengamanan Berdasarkan Sistem

Berdasarkan sistem, metode pengamanan komputer terbagi dalam beberapa bagian antara lain :

1. **Network Topology**
   Sebuah jaringan komputer dapat dibagi atas kelompok jaringan eksternal (Internet atau pihak luar) kelompok jaringan internal dan kelompok jaringan eksternal diantaranya disebut DeMilitarized Zone (DMZ). - Pihak luar : Hanya dapat berhubungan dengan host-host yang berada pada jaringan DMZ, sesuai dengan kebutuhan yang ada. - Host-host pada jaringan DMZ : Secara default dapat melakukan hubungan dengan host-host pada jaringan internal. Koneksi secara terbatas dapat dilakukan sesuai kebutuhan. - Host-host pada jaringan Internal : Host-host pada jaringan internal tidak dapat melakukan koneksi ke jaringan luar, melainkan melalui perantara host pada jaringan DMZ, sehingga pihak luar tidak mengetahui keberadaan host-host pada jaringan komputer internal.

2. **Security Information Management**
   Salah satu alat bantu yang dapat digunakan oleh pengelola jaringan komputer adalah Security Information Management (SIM). SIM berfungsi untuk menyediakan seluruh informasi yang terkait dengan pengamanan jaringan komputer secara terpusat. Pada perkembangannya SIM tidak hanya berfungsi untuk mengumpulkan data dari semua peralatan keamanan jaringan komputer tapi juga memiliki kemampuan untuk analisa data melalui teknik korelasi dan query data terbatas sehingga menghasilkan peringatan dan laporan yang lebih lengkap dari masing-masing serangan. Dengan menggunakan SIM, pengelola jaringan komputer dapat mengetahui secara efektif jika terjadi serangan dan dapat melakukan penanganan yang lebih terarah, sehingga organisasi keamanan jaringan komputer tersebut lebih terjamin.

3. IDS / IPS

Intrusion detection system (IDS) dan Intrusion Prevention system (IPS) adalah sistem yang digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari serangan pihak luar atau dalam. Pada IDS berbasiskan jaringan komputer , IDS akan menerima kopi paket yang ditujukan pada sebuah host untuk selanjutnya memeriksa paket-paket tersebut. Jika ditemukan paket yang berbahaya, maka IDS akan memberikan peringatan pada pengelola sistem. Karena paket yang diperiksa adalah salinan dari paket yang asli, maka jika ditemukan paket yang berbahaya maka paket tersebut akan tetap mancapai host yang ditujunya.Sebuah IPS bersifat lebih aktif daripada IDS. Bekerja sama dengan firewall, sebuah IPS dapat memberikan keputusan apakah sebuah paket dapat diterima atau tidak oleh sistem.

Apabila IPS menemukan paket yang dikirimkan adalah paket berbahaya, maka IPS akan memberitahu firewall sistem untuk menolak paket data itu.

Metode Deteksi IDS/IPS

Dalam membuat keputusan apakah sebuah paket data berbahaya atau tidak, IDS dan IPS dapat menggunakan metode

- **Signature based Intrusion Detection System :**

  Telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak.

- **Anomaly based Intrusion Detection System :**

  Harus melakukan konfigurasi terhadap IDS dan IPS agar dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Paket anomaly adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut.

- **Port Scanning**

  Metode Port Scanning biasanya digunakan oleh penyerang untuk mengetahui port apa saja yang terbuka dalam sebuah sistem jaringan komputer. Cara kerjanya dengan cara mengirimkan paket inisiasi koneksi ke setiap port yang sudah ditentukan sebelumnya. Jika port scanner menerima jawaban dari sebuah port, maka ada aplikasi yang sedang bekerja dan siap menerima koneksi pada port tersebut.

- **Packet Fingerprinting**

  Dengan melakukan packet fingerprinting, kita dapat mengetahui peralatan apa saja yang ada dalam sebuah jaringan komputer. Hal ini sangat berguna terutama dalam sebuah organisasi besar dimana terdapat berbagai jenis peralatan jaringan komputer serta sistem operasi yang digunakan.

Computer Security dalam Kehidupan

Computer security yang berkaitan dengan kehidupan sehari-hari, adalah sebagai berikut:

1. Keamanan eksternal / external security

   Berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran /kebanjiran.

2. Keamanan interface pemakai / user interface security

   Berkaitan dengan indentifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan

3. Keamanan internal / internal security

   Berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.

Masalah penting di kehidupan sehari-hari yang harus diperhatikan dalam keamanan komputer :

a) Kehilangan data / data loss

   Masalah data loss dapat disebabkan oleh :

   - Bencana
   - Kesalahan perangkat lunak dan perangkat keras
   - Kesalahan manusia / human error

b) Penyusup / intruder

   Penyusup bisa dikategorikan kedalam dua jenis :

   - Penyusup pasif yaitu membaca data yang tidak terotorisasi (tidak berhak mengakses)
   - Penyusup aktif yaitu mengubah susunan sistem data yang tidak terotorisasi.

Selain itu ancaman lain terhadap sistem keamanan komputer bisa dikategorikan dalam empat macam :

1. Interupsi / interruption

   Sumber daya sistem komputer dihancurkan sehingga tidak berfungsi. Contohnya penghancuran harddisk atau pemotongan kabel. Ini merupakan ancaman terhadap ketersediaan.

2. Intersepsi / interception

   Orang yang tak diotorisasi dapat masuk / mengakses ke sumber daya sistem. Contohnya menyalin file yang terotorisasi. Ini merupakan ancaman terhadap kerahasiaan.

3. Modifikasi / modification

   Orang yang tak diotorisasi tidak hanya dapat mengakses tapi juga mengubah,merusak sumber daya. Contohnya mengubah isi pesan, atau mengacak program. Ini merupakan ancaman terhadap integritas

4. Fabrikasi / fabrication

   Orang yang tak diotorisasi menyisipkan objek palsu ke dalam sistem. Contohnya memasukkan pesan palsu, menambah data palsu. Dari kategori yang ada diatas dan jika dikaitkan dalam kehidupan sehari-hari pasti kita akan menemukan masalah dalam komputer.

Ancaman Sistem Keamanan Komputer

Dibawah ini merupakan nama-nama ancaman yang sering dilihat dalam sistem keamanan komputer.

- Adware
- Backdoor Trojan
- Bluejacking
- Bluesnarfing
- Boot Sector Viruses
- Browser Hijackers
- Chain Letters
- Cookies
- Denial of Service Attack
- Dialers
- Document Viruses
- Email Viruses
- Internet Worms
- Mobile Phone Viruses

Jenis Ancaman Keamanan Komputer

Berikut ini adalah contoh ancaman-ancaman yang sering dilihat :

- Virus
- Email Virus
- Internet Worms
- Spam
- Trojan Horse
- Spyware
- Serangan Brute-force

B. Keamanan Sistem Komputer dari Perspektif Sistem Operasi

Overview

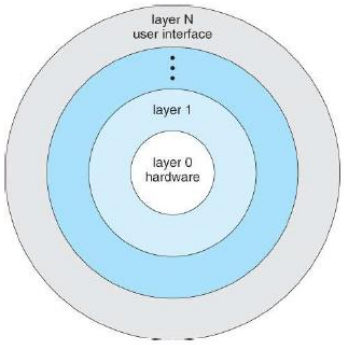
- Banyak serangan yang dilakukan bersifat silent dan invisible.
- Jika serangan dapat dilihat oleh korban, korban dapat melakukan countermeasure terhadap serangan tersebut
- Sistem operasi merupakan garis pertahanan paling depan untuk berbagai jenis kegiatan yang tidak diinginkan
- Sistem operasi harus dapat menjamin agar tidak ada proses yang tidak terautorisasi yang dapat mempengaruhi sistem yang ada
- Sistem operasi adalah control dasar dari seluruh resource dalam sistem, sehingga sistem operasi merupakan target penyerangan utama

Struktur OS

Untuk setiap mesin komputasi, sistem operasi ada di dalamnya.

- Dedicated device
- Automobile
- Smartphone
- Aplikasi Network
- Kontroller Web Server bank
- Komputer network traffic management

Berikut adalah layer struktur sistem operasi :



- Layer 5 : User Programs
- Layer 4 : Buffering for I/O
- Layer 3 : Process Management
- Layer 2 : Memory Management
- Layer 1 : CPU Scheduling
- Layer 0 : Hardware

Fitur sistem operasi berkaitan dengan keamanan sistem :

- Synchronization
- Concurrency
- Control
- Deadlock Management
- Communication
- Accounting

Fungsi OS yang membutuhkan keamanan

- Enforced Sharing
  - Resource yang ada harus dijaga integritas dan konsistensinya
  - Tabel lookup dikombinasikan dengan integrity control seperti monitoring
- Interprocess communication and synchronization
  Proses harus saling melakukan komunikasi dan sinkronisasi
- Protection of critical operating system data
  Data penting harus dilindungi dari akses yang tak terkendali (read, modify,delete)
- Guaranteed Fair Service
  CPU usage dan service lainnya harus terjaga, jangan sampai starvation terhadap service yang ada
- Interface to hardware
  Semua user harus dapat mengakses hardware, dan harus dapat berfungsi dengan benar
- User Authentication
  OS harus dapat mengidentifikasi user nya!
- Memory Protection
  - Setiap program yang dimiliki user harus memiliki bagian di dalam memory
  - Memory dapat dioperasikan oleh mekanisme dari hardware, seperti paging atau segmentasi
- File dan I/O Access Control
  Proteksi data biasanya didapatkan dari hasil lookup table yang dilengkapi dengan matriks akses control
- Allocation dan Access Control to General Objects
  Melindungi resource untuk objek lainnya yang besifat umum

History OS

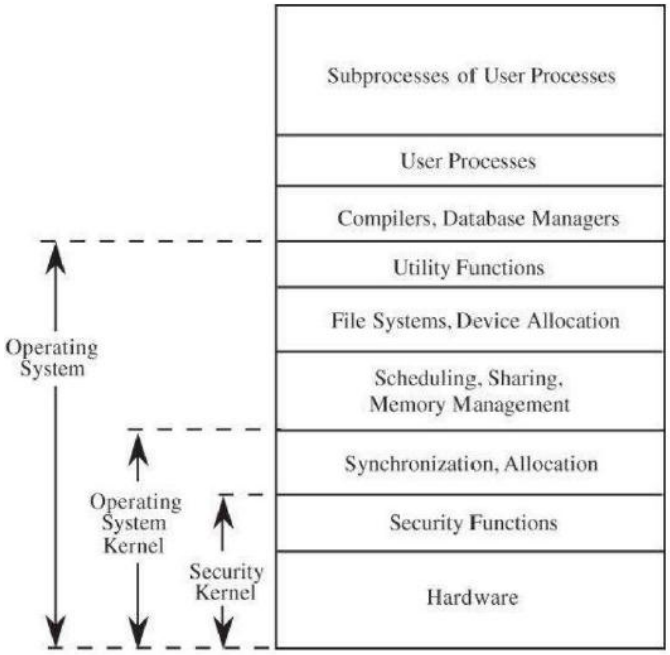
1. Single User
   - Tidak ada OS
   - User memasukkan programnya langsung ke mesin dengan menggunakan switch (atau plakat)
   - User memiliki hak ekslusif terhadap penggunaan computer sehingga user harus mengatur sendiri blocking sistem, loading libraries, dan cleaning computer
   - 1 thread
2. Multiprogramming dan Shared Use
   - Dukungan dari prosesor yang cepat
   - Permintaan user yang tinggi
   - Kapasitas yang besar

- OS digunakan untuk mempermudah sistem
- Sharing dapat menimbulkan masalah apabila tidak terdapat komunikasi antar proses

3. Multitasking
   - User dapat menjalankan beberapa proses
   - OS mengatur perpindahan (alokasi, dealokasi, realokasi) antar proses
   - OS melakukan perubahan secara cepat antar thread, sehingga tampak seperti eksekusi parallel

Desain Sistem Operasi

OS harus dapat :
- Protects Objects : OS harus melindungi beberapa objek yang ada pada komputer
- Self-Protection : OS harus dapat mempertahankan dirinya



Protected Objects

- Memory
- Sharable I/O (disk)
- Serially reusable I/O devices (printer)
- Sharable program dan subproseur
- Networks
- Sharable data

Implementasi Security pada OS

- Log adalah data yang penting
- Audit log dapat menjelaskan apa yang terjadi dari sebuah kejadian
- Analisis dari log tersebut dapat menahan dari serangan yang hampir serupa kemudian

Virtualisasi

- Mendukung kemunculan resource yang ada dengan menggunakan resource yang berbeda
  Contoh :
  Jika kita memberikan kue kepada anak-anak, kue akan habis seketika, tetapi, jika kue tersebut disembunyikan, dan diletakkan sedikit-sedikit, maka anak-anak membutuhkan waktu untuk menghabiskannya.

- OS juga dapat melakukan hal yang sama

Virtual Machine

- Apabila terdapat sekumpulan user (A&B)
- User A hanya diizinkan untuk mengakses data A.
- User B tidak dapat melihat data A, begitu pula sebaliknya
- Hal ini mudah diimplementasi dan handal dengan dua buah mesin yang tidak terkoneksi
- Mesin A dan B kita sebut dengan mesin virtual
- Dapat diimplementasi dengan menggunakan hypervisor, sandbox, honeypot

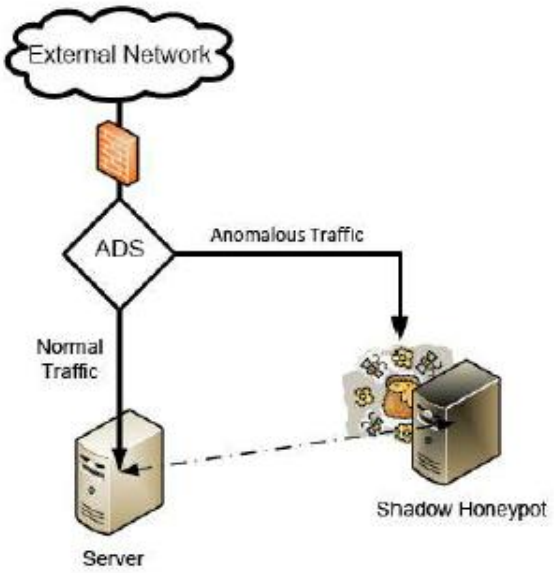
Sandbox

- Sebuah environment dimana proses yang ada terbatas, dapat terkontrol dengan menggunakan resource dari luar sistem
- Sandbox berjalan sesuai dengan keadaan sistem aslinya, kerusakan pada sandbox pada saat sebuah malicious program berjalan, tidak akan berdampak ke sistem aslinya.

Contoh : paypal sandbox, JVM

Honeypot

- Sistem yang ditujukan untuk memancing attacker untuk diserang, karena environment yang ada pada sistem (palsu) ini dapat dikontrol dan dapat dimonitor
- Ketika attacker menyerang sistem, administrator memantau kegiatan attacker dan dapat melakukan skema pertahanan terhadap serangan yang serupa.



Rootkit

- Sekumpulan tools atau program yang dapat meng-enable kan level administrator untuk melakukan akses ke computer atau ke jaringan computer
- Biasanya cracker melakukan instalasi rootkit pada computer setelah mendapatkan akses ke level user, dengan cara eksploitasi dengan cara known vulnerability atau pun cracking password
- Ketika rootkit sudah terinstall, attacker dapat melakukan masking intrusion dan mendapatkan root atau akses priviledge ke computer, atau mesin lain yang ada pada network.
- Rootkit dapat pula bekerja dengan konsep modifikasi

Modifikasi

- Patching
  - Executable code terdiri dari statement yang berupa data bytes
  - Byte tersebut tersusun dengan urutan spesifik
  - Logic dapat dimodifikasi dengan mengubah byte tersebut
- Easter Eggs
  - Logika diatas □, dapat saya dimodifikasi secara “built in”
  - Programmer meletakkan backdoor di program yang dibuat nya
  - Backdoor ini undocumented design, software ini memiliki fitur rahasia

  Contoh : Earlier versions of the widely used program Microsoft Excel contained an easter-egg that allowed a user who found it to play a 3D firstperson shooter game similar to Doom
- Spyware Modifications
  - Modifikasi spyware dan menjadikannya rootkit.
  - Spyware sulit dideteksi, begitu pula rootkit
- Source-Code Modification
  - Programmer dapat memasukkan malicious lines ke dalam program yang ada
  - Aplikasi untuk militer banyak tidak menggunakan aplikasi yang berbasis opensource
  - Open-source mendefinisikan siapapun boleh melakukan modifikasi aplikasi
  - Siapapun itu bisa saja merupakan orang yang tidak dikenal

Rootkit ≠ Exploit

- Rootkit biasanya digunakan dalam proses exploit
- Setelah attacker sukses melakukan exploit, attacker menanamkan rootkit ke dalam sistem
- Rootkit mengincar kernel dalam sistem
- Salah satu cara menginstall rootkit, dapat dilakukan dengan cara menanamkannya ke software exploit

Rootkit ≠ Virus

- Virus adalah program yang menyebarkan dirinya secara otomatis, dan tidak terkontrol
- Rootkit berada penuh dibawah control dari attacker
- Pembuatan dan penyebaran virus biasanya berada diluar control pembuatnya, sedangkan rootkit dapat dipastikan menyebar ke beberapa target tertentu.
- Untuk kasus tertentu, penyebaran rootkit hanya boleh disebarkan ke target yang terdaftar saja. Apabila disebarkan ke target yang didaftarkan, attacker (pentester) dapat terkena kasus hukum.
- Walaupun rootkit tidak sama dengan virus, teknik yang digunakan pada rootkit, dapat diimplementasikan dengan mudah pada virus.
- Ketika rootkit digabungkan dengan virus, sebuah teknologi berbahaya akan muncul

- Programmer virus menggunakan rootkit u ntuk “memanaskan” virus yang dibuatnya
- Beberapa jam awal pada saat virus disebarkan, jutaan computer terinfeksi.

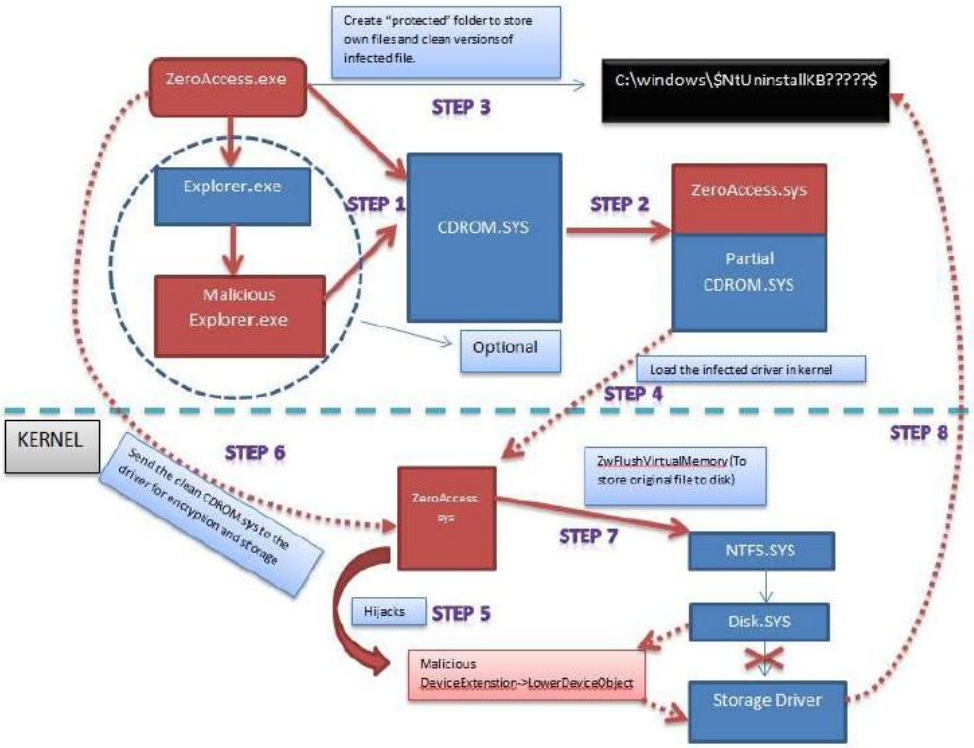
Cara Kerja Rootkit

- Hiding Mechanisms
  - Rootkit bekerja secara tersembunyi
  - Dapat menghapus log attacker saat masuk ke atau keluar dari sistem
  - Dapat menyembunyikan file dan folder yang attacker
- Backdoor Mechanisms
  - Melalui SSH connections

Komponen OS yang diserang

• I/O Manager: Logging keystrokes or network activity.
• Device & file system drivers: Hiding files.
• Object Manager: Hiding process/thread handles.
• Security Reference Monitor: Disable security policies.
• Process and thread manager: Hiding processes and threads.
• Configuration manager: Hiding registry entries

ZeroAccess



Gambar. ZeroAccess Attack

- ZeroAccess adalah salah satu rootkit yang paling banyak dibicarakan. Termasuk salah satu rootkit paling kompleks dan sangat lazim yang kami temui, dan terus berkembang.
- Rootkit ZeroAccess didistribusikan melalui rekayasa sosial dan eksploitasi.
  Posting blog baru-baru ini oleh kolega kami di McAfee menjelaskan beberapa metode aneh yang diadopsi rootkit ini untuk diinstal pada mesin tanpa diketahui.
- Salah satu tujuan dari rootkit ini adalah untuk menciptakan botnet peer-to-peer yang kuat, yang mampu mengunduh malware tambahan pada sistem yang terinfeksi. Botnet ini dilaporkan terlibat dalam penipuan klik, mengunduh aplikasi antivirus jahat, dan menghasilkan spam.

Phone Rootkit

- Rootkit dapat menyerang segala jenis OS, termasuk OS pada mobile phone
- Dalam sebuah riset, sebuah rootkit dapat menghidupkan mic pada sebuah handphone tanpa sepengetahuan user.
- Jika hal tersebut dilakukan, maka mudah bagi attacker untuk melakukan pengiriman message tersembunyi dari/ke attacker, aktifkan gps, Bluetooth, flashlight, dsb.

Contoh Phone Rootkit

- CarrierIQ : logging user keystrokes, recording telephone calls, storing text messages, tracking location
- Trevor Eckhart : logging is being done on phone and where data is going
- FinFisher-FinSpy : Remot monitoring solution which used by goverments, agencies and companies. Used for gather information from individuals and organizations.

Bagaimana Phone Rootkit menginfeksi mobilephone lain?

- Menggunakan aplikasi yang terinfeksi
- Melalui update
- Serangan baseband

Bagaimana menghindarinya?

- Latency
- Paranoid
- Cek asal aplikasi, dan yakinkan aplikasi berasal dari penyedia yang terpercaya

Rootkit Prevention

- Prophylactic Measures
  Implementasi IPS sederhana
- Configuring Systems Appropriately and Limiting Services that Run on Systems
  Hardening system dengan melakukan konfigurasi keamanan sistem
- Adhering to the Least Privilege Principle
  Melakukan privilege sampai dengan user level terbawah

- Deploying Firewalls
  - Rootkit adalah aplikasi special yang digunakan attackers
  - Firewall bertahan untuk serangan layer aplikasi (Layer 7), sehinnga dapat melakukan peningkatan kemampuan untuk identifikasi dan intercept serangan rootkit
- Using Strong Authentication
  → Gunakan shared key, Kerberos, Public Key Infrastructure
- Performing Security Maintenance on Systems
  → lakukan rutin
- Limiting the Availability of Compilers

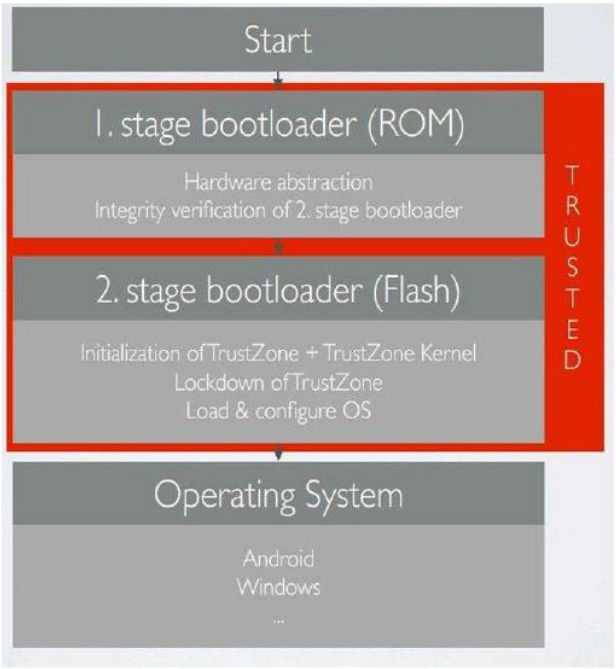
Implementasi Prevention Rootkit

- ARM Processor merupakan 32-bit RISC Processor
- TrustZone pada ARM, merupakan secure chip yang mengatur prosesor agar dapat masuk ke “mode aman”
- TrustZone :
  - Secure akses ke layar, keyboard, dan perangkat lainnya
  - Proteksi terhadap malware, Trojan, dan rootkit
  - Membuat environment yang aman (Trusted Execution Environments)
  - Membagi CPU menjadi 2 (Secure dan normal)
  - Komunikasi antar bagian CPU melalui shared memory mapping

Trusted Execution Environments

- OS yang berjalan pada TrustZone
  Contoh penerapan TEEs ada pada Netflix
- Netflix :
  - Membutuhkan device certification
  - Untuk SD, perangkat hanya membutuhkan kecepatan untuk memutar video
  - Untuk HD, dibutuhkan end-to-end DRM, sehingga video tidak dapat dicuri setiap saat
  - Video decoding dilakukan di TrustZone dengan akses langsung ke layar, tidak dapat direkam menggunakan android

Trusted Zone



Conclusion

- OS harus sanggup bertahan, mempertahankan object yang ada, dan dapat melindungi dirinya sendiri
- Rootkit merupakan bukti bahwa apabila OS yang dimiliki lemah, gaining access ke user level administrator akan mudah, dan seluruh sistem berada dibawah kendali attacker.