Keamanan Sistem Komputer

Security in OS, Rootkit

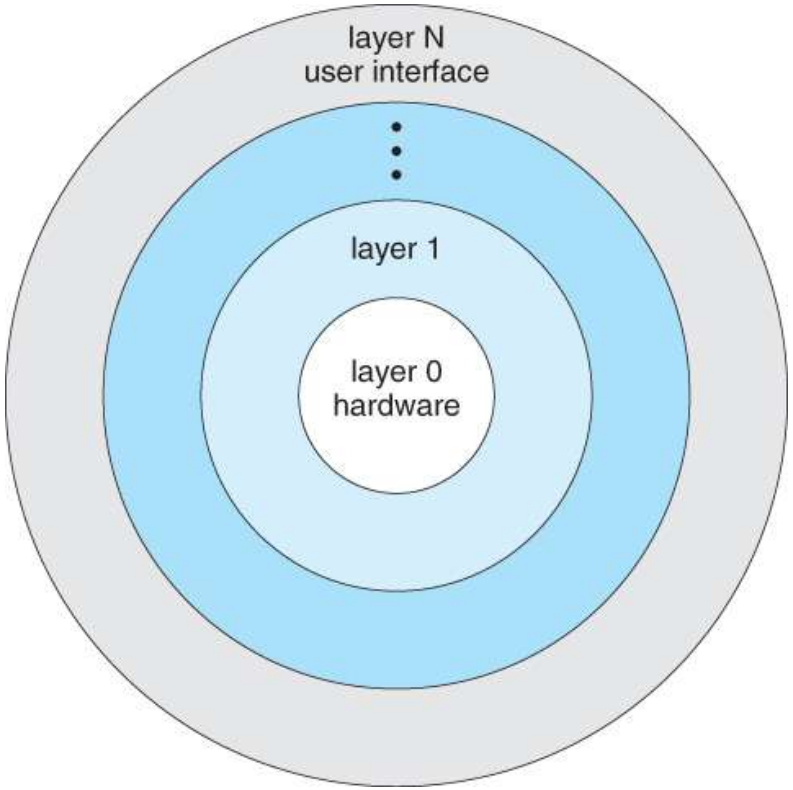
Overview

- 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

Layered Structure of the OS



- 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 OS

- 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)

Fungsi OS yang membutuhkan keamanan

- 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!

Fungsi OS yang membutuhkan keamanan

- 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 kontrol
- Allocation dan Access Control to General Objects
  - Melindungi resource untuk objek lainnya yang besifat umum

History OS

- 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

History OS

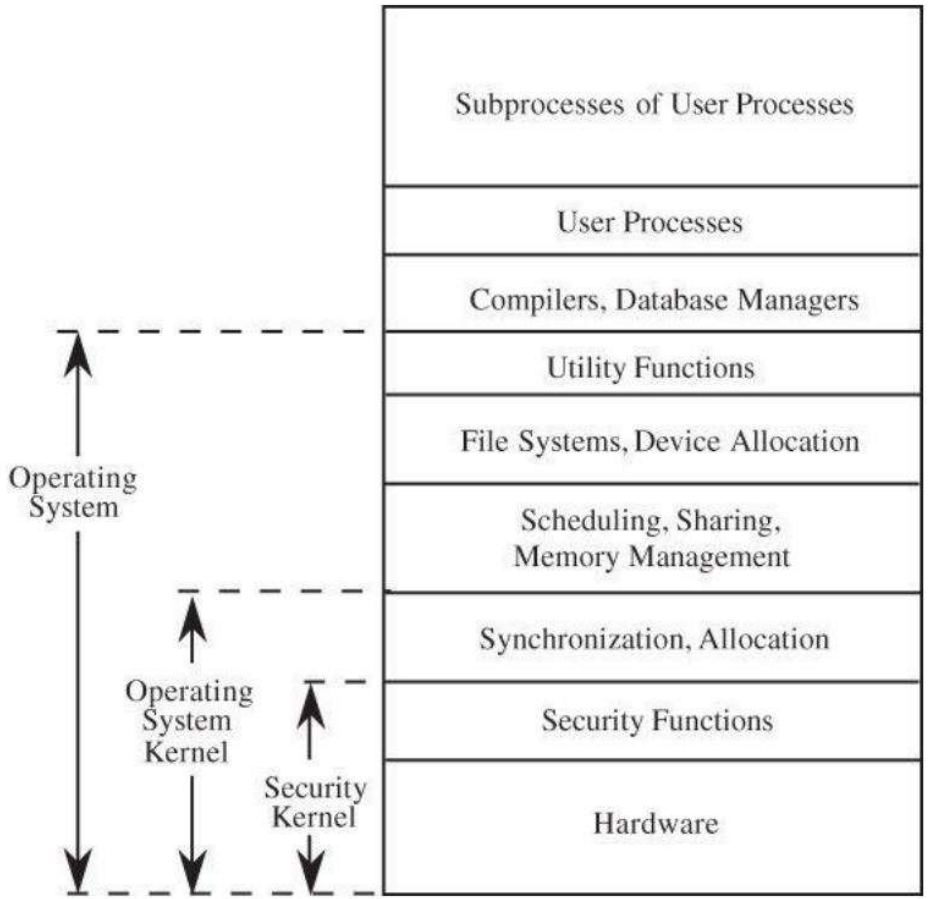
- Multiprogramming dan Shared Use
  - Dukungan dari prosesor yang cepat
  - Permintaan user yang tinggi
  - Kapasitas yang besar
  - OS digunakan untuk mempermudah sistem
  - Sharing dapat menimbulkan masalah apabila tidak terdapat komunikasi antar proses

History OS

- 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 OS

- 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

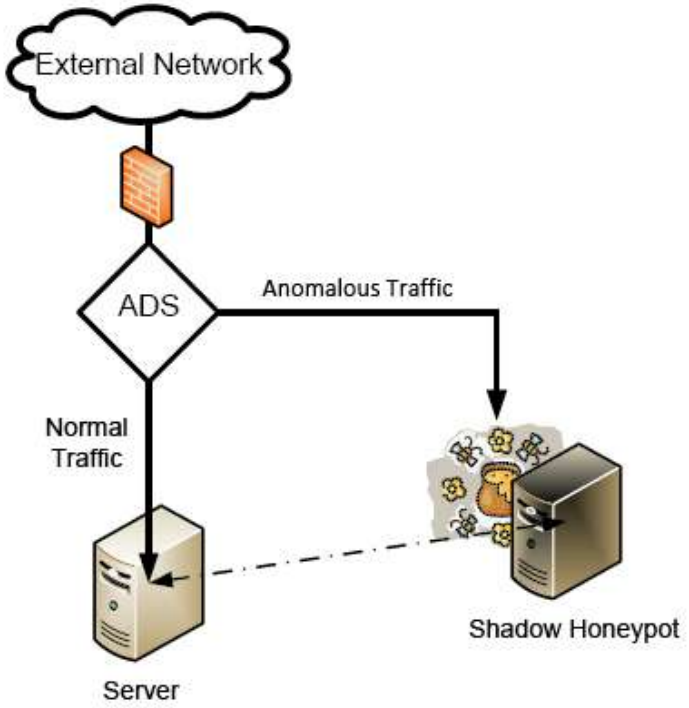
Sandbox

- 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



http://www.bluekaizen.org/rootkits-a-deeper-look/

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 first-person shooter game similar to Doom*

Modifikasi

- 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 open-source
  - 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.

Rootkit ≠ Virus

- 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 untuk “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

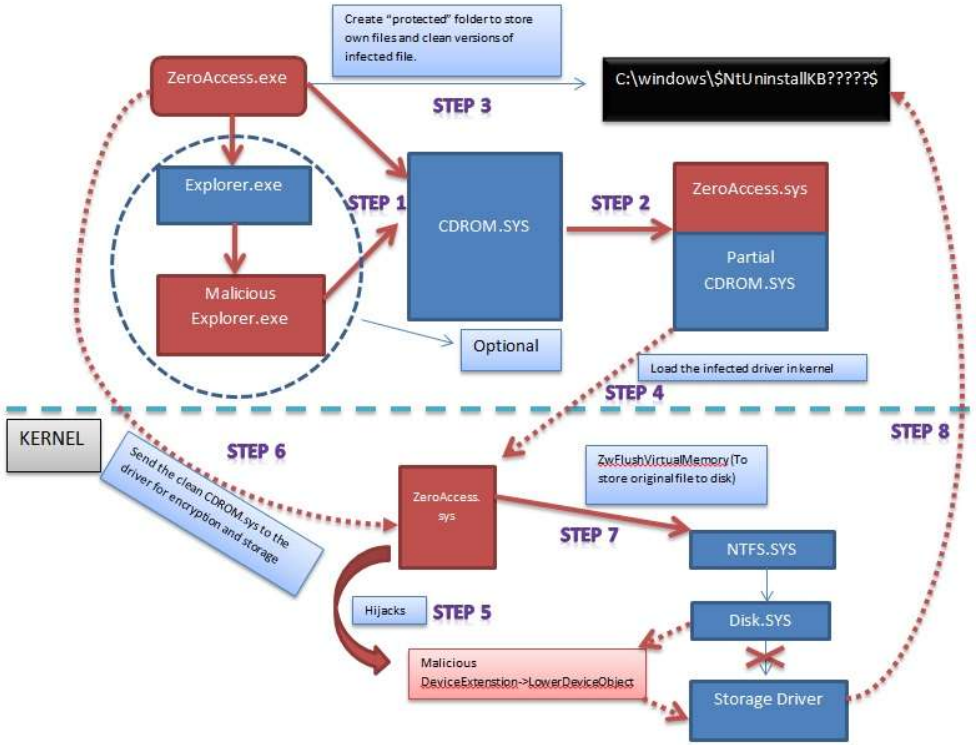
- ZeroAccess is one of the most talked and blogged, about rootkits in recent times. It is also one of the most complex and highly prevalent rootkits we have encountered, and it is continuing to evolve. The ZeroAccess rootkit is distributed via both social engineering as well as by exploitation. A recent blog post by our colleagues at McAfee describes some of the odd methods this rootkit adopts to get installed on machines without getting noticed.
- One of the goals of this rootkit is to create a powerful peer-to-peer botnet, which is capable of downloading additional malware on the infected system. This botnet is reportedly involved in click fraud, downloading rogue antivirus applications, and generating spam.

https://blogs.mcafee.com/mcafee-labs/targeting-zeroaccess-rootkits-achilles-heel/

ZeroAccess

https://blogs.mcafee.com/mcafee-labs/targeting-zeroaccess-rootkits-achilles-heel/

ZeroAccess Attack



https://blogs.mcafee.com/mcafee-labs/targeting-zeroaccess-rootkits-achilles-heel/

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.

Example of 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.

Phone Rootkit

- Bagaimana 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

Rootkit Prevention

- 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

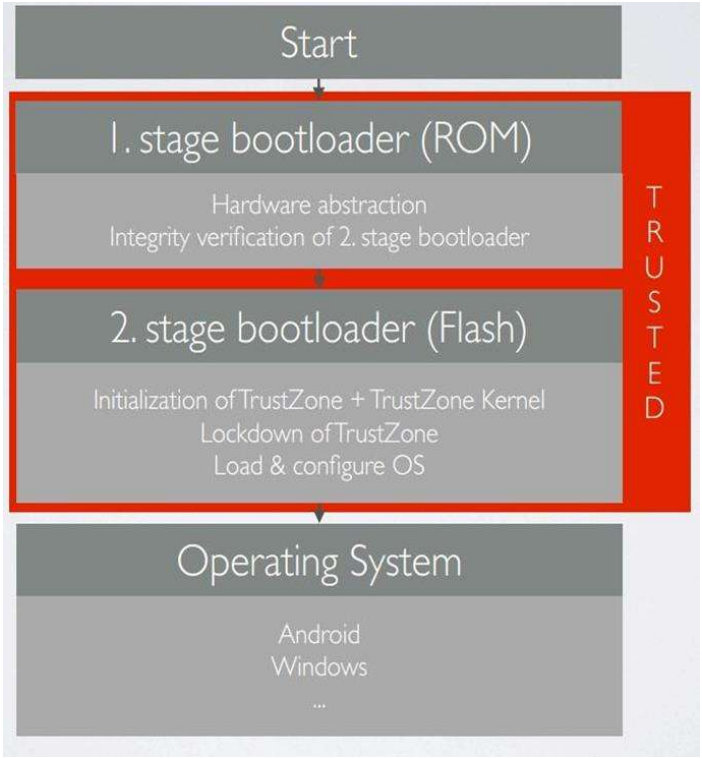
Implementasi Prevention Rootkit

- 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



http://resources.infosecinstitute.com/rootkits-on-your-smartphone/

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.