Tugas Mobile Computing

An Android Application Sandbox System For Suspicious Software Detection

Oleh

Dimas Adityo

2210205005

An Android Application Sandbox System For

Suspicious Software Detection

Abstrak

Kepopuleran Smartphone menggunakan sistem operasi Android saat ini telah banyak dimanfaatkan oleh berbagai kalangan. Meskipun menggunakan basis Sistem Operasi Linux, Banyak aplikasi android yang saat ini bisa diunduh secara bebas, android memiliki property yang dapat dimanfaatkan oleh pihak lain tanpa Sepengetahuan pihak pengguna. Melalui penelitian ini dicoba teknik dalam menganalisa aplikasi dari pihak ke-3 dengan nama "Android **Application Sandbox (AASandbox)**", Aplikasi ini berjalan melakukan analisa secara ***Statis*** dan ***Dinamis*** , semuanya bekerja secara otomatis dan bersamaan dalam mendeteksi aplikasi yang dicurigai mengandung malware. Analisa Statis melakukan scanning aplikasi secara online(tanpa menginstall pada device). Analisa Dinamis melakukan scanning melalui devices dengan kemampuan mengakses sumberdaya hingga pada level low format. Keduanya dapat dideploy melalui jaringan cloud computing,sehingga distribusinya dapat dilakukan secara cepat dalam menggantikan peran fungsi antivirus model klasik.

1. PENDAHULUAN

Metode scanning virus yang saat ini banyak dilakukan ialah dengan menganalisa pola dan kebiasaan cara kerja virus kemudian menyimpan pola – pola tersebut kedalam database,meskipun pada beberapa virus yang ada terlewati untuk dapat dideteksi .Masalah lain yang biasanya terjadi ialah waktu untuk melakukan analisa dan mengupdate database dibutuhkan 48jam,artinya peluang terjadinya serangan dari malware berikutnya sangat mungkin dilakukan apabila sebuah sebuah smartphone tidak segera mengupdate antivirusnya. Terdapat metode sandbox antara lain CW Sandbox atau JAVA Sandbox.

2. Related Work

2.1 Sekuriti Pada SmartPhone Android

Membandingkan security pada perangkat mobile dengan PC sangat berbeda, pada smartphone banyak sekali aspek yang mempengaruhi, diantara-nya ialah mobile Infrastrukture (didalam-nya terdapat informasi Billing) sehingga menarik sekali bagi para penyerang (attacker) untuk berlomba memperoleh informasi ini. Mekanisme untuk melakukan pertahanan ini banyak dilakukan, meskipun sulit beberapa penelitian telah menunjukkan hasil yang menakjubkan. Meskipun Android merupakan sistem operasi mobile yang masih baru,beberapa publikasi terkait masalah sekuriti pada mobile android telah banyak didiskusikan antara lain, **1**.Mekanisme keamanan pada Android,**2.**Malware Detection, **3.**Analisa pada *Application Permision*. Dan issue pada **4.***Kernel Hardenin.*

2.2 Teknik Analisa software secara statis Vs SandBoxing

Untuk melakukan deteksi malware terdapat dua cara yaitu dengan melalui analysis secara Statis maupun Dinamis. Analisa statis melibatkan proses binary forensic termasuk didalamnya ialah decompilation,decryption, patern matching. Analisa Dinamis ialah teknik analisa yang melibatkan sebuah proses control terkait dengan lingkungan,kebiasaan. Biasanya digunakan dalam melakukan

monitoring terhadap perubahan Files, Aktifitas Jaringan, processes dan threads, system call tracing. Analisa dinamis membutuhkan algoritma yang lebih kompleks daripada analisa statis. Pendekatan teknik analisa yang lain ialah dengan Teknik *SandBoxing*. Teknik ini membatasi setiap proses dengan kebijakan keamanan yang telah ditentukan.Beberapa design dan implementasi dari aplikasi sandbox yang ada salah satunya ialah dengan teknik CWSandbox.

3. Aplikasi Sandbox Android

Sandboxs biasanya ditempatkan kedalam lokasi sebuah kernel,Kernel merupakan bagian yang sangat esensial dari sebuah sistem,karena kernel merupakan jembatan antara hardware dengan software. Salah satu pendekatan sistem sandbox ialah untuk melakukan monitoring system dan library termasuk didalamnya argument.

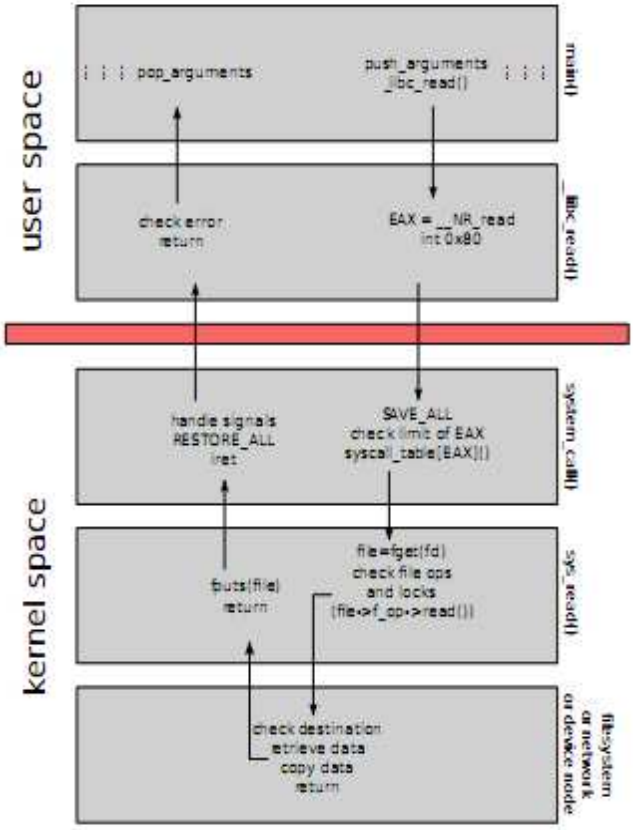

Figure 2. Steps involved in performing a `read()` system call from user space (derived from [26]). Each arrow in the figure represents a jump in the instruction flow.

4. Analisa Statis Dan Dinamis Pada Aplikasi Android

Pada teknis analisa ini menggunakan 2 langkah model pendekatan terbaru, terdiri atas sebuah **full fledged kernel space sandbox** dan **sebuah fast static pre-check.** AASandbox bekerja secara otomatis tanda campur tangan manusia, kemudia AAsendbox Log dan system calls serta analisa dinamis untuk investigasi selanjutnya.

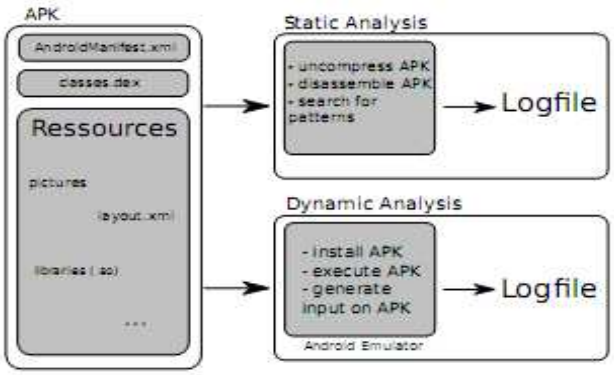

Figure 3. Design of the Android Application Sandbox (AASandbox). AASandbox consists of three main parts: the APK, static and dynamic analysis methods, and resulting dataset for further analysis.

4.1 **Analisa Statis pada Aplikasi Android**

Sebuah android application Package (APK) digunakan untuk menganalisa pola khusus (Runtime.exec()). Decompression: Sebuah aplikasi android menggunakan kompresi (ZIP), ketika di uncompress file ini tediri atas 3 bagian utama didalam direktori bernama :

APK-NAME /Unzipped/:

-. AndroidManifest.xml, sebuah file xml berisi meta data informasi tentang aplikasi,Description, Security Permision dsb.

-. Classes.Dex, Sebuah file tunggal yang berfungsi untuk membawa informasi bytecode yang akan di interpreted menggunakan Dalvik VM.

-.Res/, Sebuah folder yang terdiri atas definisi layout,Bahasa dsb.

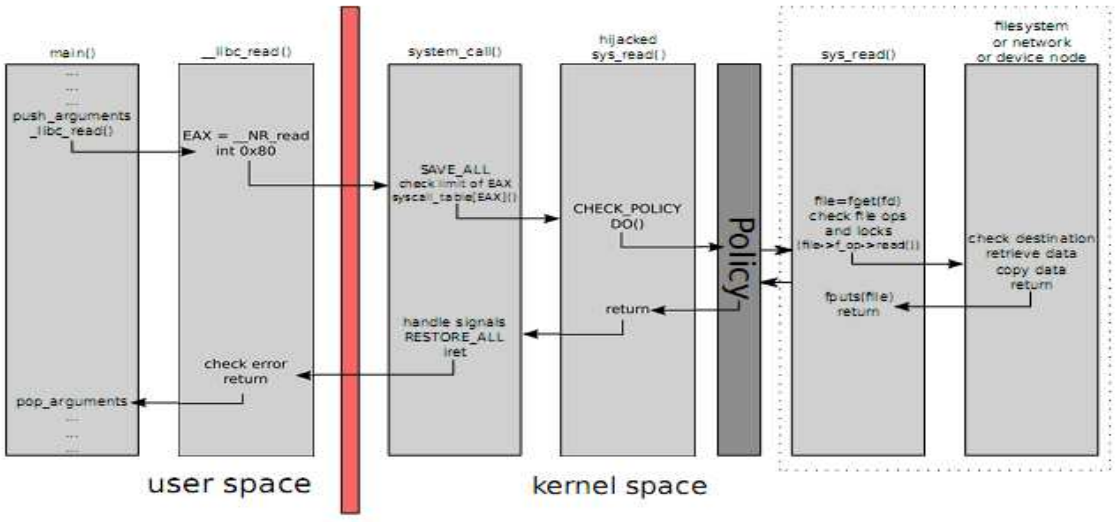

Figure 1. Steps involved in performing a hijacked read() system call. The procedure on the first steps is similar to Figure 2 up to the step when the hijacked read() system call routine arrives. There, the further processing is described by the policy and depends on the implementation of the system call itself.

Dekompilasi Search ,

File classes.dex menyimpan aplikasi bytecode, file ini dikonversi kedalam format yang bisa dibaca menggunakan baksmali, yang akan menghasilkan sebuah java folder terdiri atas beberapa file yang bisa di parsing dengan mudah.

Patern Search,

Langkah yang terakhir, kode yang telah disassembled bisa di scan untuk mendapatkan pola-nya.Selanjutnya sistem akan mencari bagian mana yang kira – kira dicurigai mengandung konten jahat.

4.2 **Analisa Dinamis pada aplikasi android**

Untuk melakukan analisa dinamis, pertama harus disiapkan beberapa aplikasi, yaitu menyiapkan EMULATOR Android, Menginstall Paket AASandbox, dan Isntallasi APK dan Start Monkey, kemudian mendapatkan Log dari System call.

5. **Ringkasan**

Dalam penelitian ini dibuat aplikasi sandbox yang mampu melakukan analisa sebuah aplikasi sebuah layanan berbasis cloud. Dengan menambahkan Fungsi Pre Check aplikasi sandbox ini bisa menganalisa pola yang mencurigakan dengan menggunaka analisa statis. Pelacakan jejak, log, dan investigasi dilakukan secara otomatis dengan menggunakan analisa dinamis.

Referensi :

1 .M. Becher, F. Freiling, and B. Leider. On the effort to create smartphone worms in windows mobile. In Information As- surance and Security Workshop, 2007. IAW ’07. IEEESMC, pages 199–206, 20-22 June 2007.

2. J. Bergeron, M. Debbabi, J. Desharnais, M. M. Erhioui, Y. Lavoie, and N. Tawbi. Static detection of malicious code in executable programs. In Proceedings of the Symposium on Requirements Engineering for Information Security (SREIS’01), 2001.

3. M. A. Bishop. The Art and Science of Computer Security. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

4. Bundesamt f¨ ur Sicherheit in der Informationstechnik. Mobile endger¨ ate und mobile applikationen: Sicherheitsgef¨ ahrdungen und schutzmassnahmen, 2006.