FIELD NOTE / CATATAN

Procyon, Powerful Java Bytecode Decompiler

Petruknisme · 8 Apr, 2017 · 2 min to read

Tulisan yang saya buat kali ini merupakan opini pribadi, jadi mungkin isi dari tulisan ini bisa salah dan benar. Tolong koreksi bila ada kesalahan dalam pembahasan. Sebenarnya ini tulisan lama yang belum saya realisasikan kedalam tulisan. Berkisar 1 tahun lalu, disaat masih berkecimpung dalam development menggunakan Java sebagai server. Jadi, saat itu saya diharuskan melakukan reverse engineering untuk mendapatkan source code dari sebuah aplikasi java yang dimana adalah closed project. Well, saya pikir 'ah cuman java app toh banyak decompiler', tapi nyatanya? 😀

Beberapa aplikasi decompiler sudah dicoba untuk melakukan decompile terhadap project tersebut. Dari mulai JD-GUI, CFR, KRAKATAU dan lain-lain. Semua terkendala dalam translasi bytecode yang sudah di obfuscate dan dienkripsi sebelumnya. Untuk perbandingan antara tools yang dipakai bisa dilihat pada http://www.ghettoforensics.com/2013/09/malware-analysis-state-of-java-analysis.html (http://www.ghettoforensics.com/2013/09/malware-analysis-state-of-java-analysis.html) yang dimana menyuguhkan sample case. Untuk Hacking Java Bytecode sendiri bisa dibaca pada laman berikut https://www.acloudtree.com/hacking-java-bytecode-for-programmers-part1-the-birds-and-the-bees-of-hex-editing/ (https://www.acloudtree.com/hacking-java-bytecode-for-programmers-part1-the-birds-and-the-bees-of-hex-editing/)

Oke, jadi kenapa saya pilih Procyon? Well, dari hasil yang saya dapatkan dalam decompile project tersebut, terbukti bahwa procyon yang lebih akurat dalam proses decompile terutama untuk bagian bytecode yang tidak banyak bisa ditranslasi oleh JD-GUI dan kawan-kawan. Maaf saya kurang bisa dalam menjelaskan secara teknis karena memang diluarkemampuan saya.

Untuk procyon sendiri bisa didapatkan pada link berikut https://bitbucket.org/mstrobel/procyon (https://bitbucket.org/mstrobel/procyon) . Procyon merupakan Java Decompiler berbasi CLI, tapi ada juga versi GUI yang dibuat oleh orang lain https://github.com/deathmarine/Luyten (https://github.com/deathmarine/Luyten)

Ah, tulisan kali ini hanya asumsi dan sebagai catatan saja. Semoga ada manfaat yang diambil.

Catatan

Licensed under CC BY-SA 4.0