



Détecteur de virus par morphologie Morphological virus detector

Une nouvelle technologie pour reconnaître les virus dans les fichiers
A new technology to recognize files infected by computer malware.

Partenariat

Nous envisageons une collaboration avec toute société intéressée par évaluer cette innovation.

Description technique

Parmi les problèmes connus des logiciels anti-virus, il y a au moins le problème de la mise à jour incessante et la trop forte sensibilité aux mutations. De plus, pour les compagnies d'anti-virus, la maintenance du logiciel est lourde, coûteuse du fait que le travail doit être fait à la main.

Nous proposons une nouvelle caractéristique des virus que nous appelons signature morphologique. Ces signatures peuvent être construites automatiquement, elles peuvent être comprimées dans de grandes bases de données, elles peuvent également être reconnues efficacement dans les fichiers à tester.

Etat de développement

Nous avons développé un prototype, testé sur notre propre base de données de virus. Nous sommes actuellement en train de faire des tests sur des bases de données fournies par une société de logiciels anti-virus pour le compte de cette société.

Champ d'application du marché

La technologie peut être employée dans de nombreux domaines, comme les logiciels anti-virus, mais aussi les télécommunications ou les services de réseau informatique. L'administration, en particulier la Défense nationale, est aussi une cible potentielle pour l'application.

Innovation, différenciation

Les signatures morphologiques sont beaucoup plus résistantes aux mutations de malware, par conséquent, un détecteur les employant sera plus fiable. Les mises à jour sont simplifiées par l'extraction automatique, la base de données est optimisée, ce qui permet l'économie de mémoire.

Propriété intellectuelle

Patents pending : PCT/CA2005/001216



Partnership

Any company or institution interested by this innovative tool is welcomed to contact us

Technical Description

Among issues of present anti-virus software, there are at least two: they need very frequent updates and they are very sensitive to mutations of viruses. Moreover, for the company, the software maintenance is heavy: the most part of the updates are to be done manually.

We propose a new notion to characterise malware that we call morphologic signature. They can be automatically extracted from suspicious files, they can be automatically compressed into a large data-base and they can be efficiently rediscovered in some files.

Development status

We tested a beta version of the software on our own malware database, and our own selection of sane programs. We are currently making some benchmark for some anti-virus software company.

Market Application Field

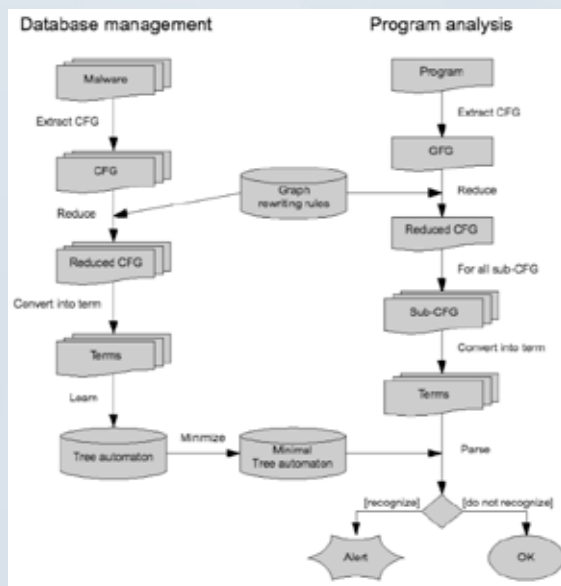
The technology can be used in a wide range of application: anti-virus software, telecommunication or networking. State administration such as Defense Services can use such a product.

Innovation, differentiation

Morphological signatures are much more resistant to malware mutations, and thus provide a more precise detector. They can be automatically synthesised, and can be efficiently compressed. Updates are simplified, and some memory is saved.

IP Status

Protected software



Pour en savoir plus / To know more

Laboratoire de Haute Sécurité LORIA
BP 239 - Vandoeuvre lès Nancy 54506
<http://lhs.loria.fr>