

## Diagnostic de sécurité des ordinateurs grand public

### Description

Les utilisateurs dans le grand public subissent aujourd'hui de plus en plus de dommages. Un projet au sein de l'institut ICT consiste à étudier cette problématique et à développer un média sous forme de site Internet permettant aux utilisateurs grand public de se sensibiliser, de se former ainsi que de tester la sécurité de leurs ordinateurs.

Ce travail de diplôme vise à concevoir et développer une partie de ce média : un diagnostic de sécurité. Des pages web devront en effet permettre à un utilisateur de déterminer le niveau de sécurité de son ordinateur en vérifiant la configuration basique de son système d'exploitation, de son *firewall* personnel et éventuellement de son antivirus (en partant du diagnostic antivirus déjà réalisé dans un autre travail de diplôme en 2004).

### Le Site Web

Le site Internet est l'interface par laquelle l'utilisateur effectue toutes les opérations. Etant donné le public cible, il se doit d'être simple d'utilisation et mettre en avant l'outil principal qu'est le diagnostic de sécurité.

L'analyse du poste de l'utilisateur concernant les connexions provenant de l'extérieur vient s'ajouter aux fonctionnalités du site. En effet, cette tâche doit s'effectuer depuis une machine distante et ne peut, par conséquent, pas être intégrée au logiciel.

Enfin, les résultats obtenus sont affichés de manière globale, puis de façon plus détaillée en fonction des choix de la personne ayant lancé le diagnostic.

### Le Logiciel

Une fois téléchargé sur le PC, le logiciel est lancé par l'utilisateur. Il teste les mises à jour du système d'exploitation, le *firewall* et l'antivirus de la machine sur laquelle il est exécuté.

L'entreprise Shavlik met à disposition sur le Web un fichier XML contenant tous les bulletins de sécurité de Microsoft. Cette source de données est analysée en fonction des caractéristiques du PC. Les mises à jour manquantes sont alors enregistrées.

Le logiciel tente ensuite d'établir plusieurs connexions sur un serveur distant. Si celle-ci peut être établie, cela implique qu'aucun *firewall* applicatif n'est installé.

Enfin, les informations concernant l'antivirus sont récupérées dans la base de registre et la présence des fichiers correspondants est vérifiée.

### Fonctionnement

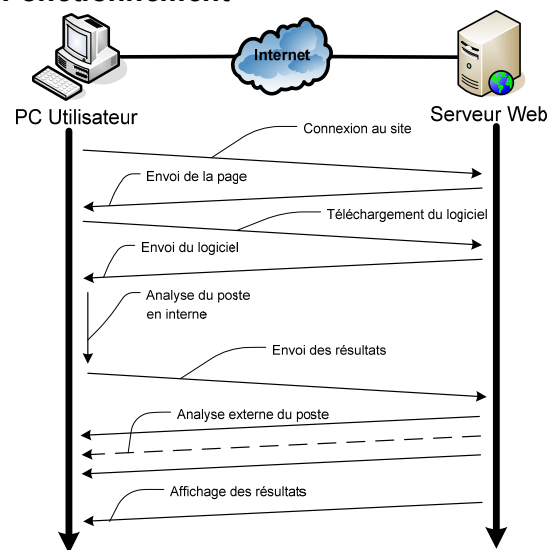


Schéma de fonctionnement du diagnostic

Ce diagnostic est compatible avec n'importe quel navigateur Internet. Le logiciel est quand à lui compatible avec les systèmes d'exploitation définis dans le cahier des charges (Windows 98, 2000 et XP).