

# GSIQ / ISSA Québec



## La sécurité adaptée à la réalité

GSIQ / ISSA

### La théorie des petits pas

Cher membres,  
L'année 2006 a été une année de changement, de rebondissement et de conférences très intéressantes. Je voulais prendre les quelques prochaines lignes pour partager avec vous le chemin que le GSIQ/ISSA a fait dans la dernière année et les grands projets que l'on vous réserve pour 2007.

L'histoire du GSIQ a commencé lorsque les gens du CHUQ sont venus me voir alors que je travaillais chez Microsoft pour me demander si on était intéressé à les aider à partir un groupe de rencontre et de discussion en sécurité informatique et parler "techno". Certains groupes existent aujourd'hui à Québec, discute gouvernance et grandes orientations, par contre, le groupe du GSIQ/ISSA est unique de par le fait que nous essayons de rester

le plus techno possible, de parler et de démontrer la technologie. Le groupe compte maintenant près de 150 membres et notre plus grand auditoire cette année fut de 52 personnes.

Le but premier du groupe est de faire grandir le bagage de connaissances en sécurité de ses membres. Nous avons eu plusieurs sessions cette année touchant le côté du "hacking" et je crois que les personnes présentes ont beaucoup appris de ces sessions, on apprend à



connaître l'ennemi et on se défend mieux par la suite. La preuve est que j'ai vu des

gens utilisé BackTrack lors du concours de hacking de septembre dernier, un outil qui avait été présenté lors d'une conférence précédente...

Mon objectif pour 2007, continuer de faire grossir le groupe, être capable de faire venir à Québec des experts en sécurité et d'augmenter le niveau commun d'expertise du groupe.

J'espère pouvoir rencontrer 2-3 nouveaux visages à chaque rencontre.

Dans les mots de Hellen Keller: "Security is mostly superstition. It does not exist in nature. Avoiding danger is no safer in the long run than outright exposure."

Donc, plus on en connaît, moins on aura besoin d'éviter le danger et plus on pourra éteindre les mythes...

*Stephane Asselin*

### Voice over IP, Risques vs bénéfiques...

Par Alain Mercier

La VoIP est de plus en plus présente dans nos organisations souvent pour des raisons économiques. Mais les aspects touchant la sécurité (tant à l'égard des menaces que des bonnes pratiques) entourant cette technologie doivent être bien intégrés à ce projet. Des menaces comme la possibilité pour un pirate d'écouter, enregistrer ou de modifier une conversation si elle n'est pas

chiffrée, les dénis de services, la manipulation des protocoles utilisés pour le VoIP (ex. : SIP), le vishing, les vulnérabilités logicielles dans les infrastructures sous-jacente, le SPIT, etc. sont présentes dans le monde du VoIP. Il faut comprendre que la téléphonie sur IP ou VoIP ne fait souvent qu'ajouter des infrastructures et applications sur nos réseaux IP existant. Du côté des bonnes prati-

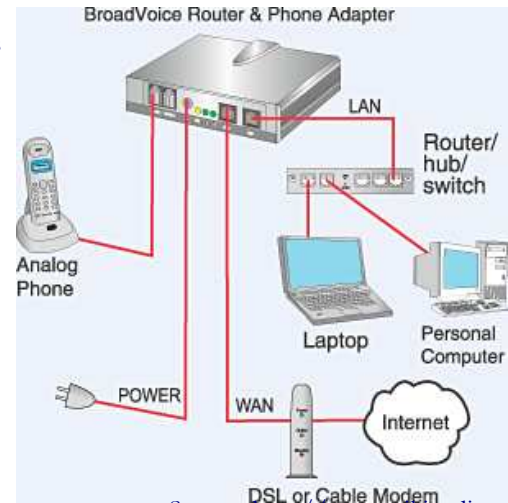
#### Dans cette parution:

VoIP	2
Outils pour Pocket PC	2
Gestion des mots de passe	2
Calendrier 2007	3
Sécurité applicative	4
Enrichir notre vocabulaire	4

## VoIP, Risques vs bénéfices, (suite)

ques à mettre en place pour prévenir et prendre en considération les menaces énoncées il faut durcir (*hardening*) les serveurs/passereaux/routeurs/pare-feu entourant le VoIP, ajuster les pare-feu (ports dynamiques du VoIP) pour SIP ou H.323, chiffrer le trafic (signalisation, contrôle et voix) pour assurer la confidentialité, avoir une redondance pour assurer la disponibilité (serveur, télécommunication, UPS, etc.), faire un audit de sécurité sur ses équipements VoIP, etc. Les fournisseurs sont plutôt préventifs en ce qui a trait à l'introduction de la sécurité dans le VoIP. Il reste toutefois qu'aucune technologie n'est exempte de risque à 100 % et il faut gérer le risque relié au VoIP.

Pour en savoir plus, vous pouvez consulter le site du CRIM dans la section de l'ISIQ,



Source: <http://www.wikipedia.org>

<https://www.isiq.ca/fr/>

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore  
From MS Technet, 10 security laws...

## Un outil pour remplacer les Post-It (<http://keepass.sourceforge.net>)

par Stéphane Asselin

Ils vous arrivent sûrement d'oublier votre mot de passe. Étant une personne travaillant en sécurité informatique, je fais face à un choix très difficile à faire, utiliser un mot de passe complexe et l'utiliser à plusieurs saucés (authentification au domaine, achat sur le web, VPN, ...) ou encore j'utilise un mot de passe différent à chaque endroit. Il y a un peu plus

de 8 ans de cela, j'ai opté pour utiliser un mot de passe différent à chaque endroit. Ceci peut causer d'énormes maux de tête étant donné la quantité monstrueuse de mots de passe utilisés. J'utilisais jusqu'à l'été dernier un fichier texte, encrypté localement. Vous pouvez deviner que ceci apporte une toute autre série de problèmes, si jamais je perds ou me fais voler ce fichier.

J'ai découvert cet été un logiciel Open Source pour conserver ces mots de passe. On peut partir un débat sur le sujet, les bénéfices ou risques de centraliser ceci mais moi, j'ai opté pour un peu plus de sécurité mais conservé à un seul endroit. Je vous invite à l'essayer et m'en donner des nouvelles.



## Quand le chat sort du sac...

Est-ce que vous pensez que votre mot de passe est sécurisé? Quelle est la longueur de votre mot de passe? Quelle est la complexité de celui-ci (3 catégories sur 4)? Quels est le maillon le plus faible dans votre mot de passe? Utilisez-vous un mot de passe que l'on retrouve dans le dictionnaire?

Ceci n'est qu'une infime partie

des questions que vous devriez vous poser lorsque vous décidez de choisir un mot de passe. Naturellement, on n'a pas besoin d'utiliser une porte en béton armé pour protéger une poignée de sable...

Je voulais vous laisser avec quelques outils qui peuvent vous aider à tester la force de votre mot de passe:



- John The Ripper ([www.openwall.com/john](http://www.openwall.com/john))
- L0phtcrack (LC5), le plus utilisé...
- Brutus (plus vieux mais toujours bon)
- [www.password-crackers.com](http://www.password-crackers.com) (site à utiliser à vos risques...)
- Cain&Abel ([www.oxid.it/cain](http://www.oxid.it/cain))

## Calendrier d'activité pour 2007

Plusieurs sujets ont été lancés pour le groupe de sécurité, nous sommes toujours à la recherche d'idées et de conférenciers pour venir nous éduquer sur le vaste domaine de la sécurité. Voici quelques-uns des sujets qui ont été retenus pour 2007:

### Janvier 2007

Retour sur l'événement de sécurité de septembre 2006 (How-To...)

### Février 2007

Présentation par le CRIM

### Mars 2007

Risking the Enterprise – New Approaches to Identifying and Managing Information Security Risk in your Business (Événement par Microsoft)

### Avril 2007

Évaluer les V.A. et les pen test...

### Mai 2007

SIM: Information overload



Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore  
From MS Technet, 10 security laws

## Outils pour Pocket PC

par Daniel Marcotte

Pour ceux qui possèdent un Pocket PC, smartphone ou un appareil utilisant Windows CE, voici deux petits logiciels fort utiles et 100% gratuits:

Vxutil permet de connaître l'adresse ip en cours d'utilisation, Port scanner, trace route, ping, ping sweep et plusieurs autres fonctions

[http://www.cam.com/vxutil\\_pers.html](http://www.cam.com/vxutil_pers.html)

WiFiFoFum est un WiFi scanner <http://www.aspecto-softwa-re.com/rw/applications/wififofum/>

Je vous recommande d'installer [.NET Compact Framework 2.0 Service Pack 1 Redistributable](#)

avant WiFiFoFum car celui qui vient avec l'installation est plus vieux.

J'utilise ces logiciels sur [un Hp Ipaq 2940b](#) et ils fonctionnent très bien. Lisez bien la section FAQ ou la description du logiciel pour être sûre que ça va fonctionner avec votre appareil. Bon sniffage...

## Évaluation de vulnérabilité (partie 1)

Un des grands défis pour une entreprise est de rester à jour à l'intérieur de son parc informatique, de savoir en tout temps ce qui se passe, d'avoir un état de situation du niveau de vulnérabilité de son parc. Plusieurs compagnies fournissent des logiciels pour évaluer ces niveaux de vulnérabilité, donne un indice et/ou un ordre de grandeur et certaines donnent

même un chiffre sur une échelle de vulnérabilité. La plus grande lacune que je vois avec ces diverses applications est qu'elle donne souvent un faux sens de sécurité. Exemple, le logiciel donnera un indice de sécurité de 4.5 sur 5 pour une évaluation d'un serveur mais ce logiciel ne tient pas compte de l'endroit physique où est stocké ce serveur, du nombre d'invidus



qui ont des droits administratifs sur le serveur et il ne tient pas compte de

l'environnement physique autour du serveur (électricité, ...). Ceci se voulait seulement une introduction, dans la partie 2, on parlera de V.A. et tous les parties à prendre en considération et des outils...

A chaque mois, nous allons mettre dans cette section une définition ou une description d'un terme fréquemment utilisé en sécurité. Nous allons également fournir des références ainsi que des liens d'intérêts.

Définition du mois: Botnet

- A botnet (or bot farm) is a network of distributed computers, made up of computers used without the owner's knowledge (also called a Zombie army)

-Typical uses:

- spam relays
- adware servers
- launch DDoS attacks
- remote disk storage for pornography sites

Liens d'intérêts:

Excellent papier allant en détail sur le sujet: <http://www.honeynet.org/papers/bots/>

Article du SANS: [http://www.sans.org/reading\\_room/whitepapers/malicious/1299.php](http://www.sans.org/reading_room/whitepapers/malicious/1299.php)



## Organization

*Stéphane Asselin, rédacteur en chef*

---

## La sécurité des applications Web par obscurcissement

Par Mario Audet

La sécurité des applications Web par obscurcissement, vous connaissez? Non? C'est pourtant une pratique populaire réalisée par certains. Cela consiste à ne pas corriger les failles de sécurité dans les applications Web et de ne pas diffuser leurs présences. Vous savez maintenant de quoi je parle et vous pensez peut-être à certaines applications Web malveillantes utilisant le *Cross site Scripting*. Détrompez-vous car il n'y a pas que ces applications Web qui peuvent contenir des failles...

### Est-ce courant cette pratique?

Dans certaines organisations, il y a des applications Web qui ont été développées à l'interne (ou par des firmes externes), qui sont fonctionnelles et dont la sécurité par obscurcissement a été appliquée. Il s'agit parfois de raccourcis pour accéder directement à une base de données ou un *backdoor* pour accéder au code source par exemple.

Selon Gartner Group, 75% du piratage informatique mondial s'est produit au niveau des applications Web en 2005. Il va s'en dire que les failles provoquées par la sécurité par obscurcissement contribuent à alimenter cette statistique. Également selon la liste du US-CERT en 2006, la majorité des 20 vulnérabilités les plus sévères sont des défauts au niveau d'applications Web. Cela veut tout dire...

### Pourquoi la sécurité par obscurcissement?

D'abord, ce genre de comportement est provoqué par certains développeurs qui n'hésitent à transgresser certaines règles de sécurité, par certains gestionnaires soucieux de ne pas provoquer de scandales et d'économiser, par la progression du RAD (Rapid Application Développement) qui incite à produire très rapidement, par la complexité des applications, par la multitude de langages de programmation et par l'absence de maintenance des applications Web.

### Que faut-il faire pour contrer cette pratique?

Quelles sont les solutions possibles à la sécurité par obscurcissement? D'abord, la sensibilisation auprès des équipes de développement et des gestionnaires est nécessaire. Les organisations doivent également ajuster leurs politiques de sécurité et réaliser différents tests pour détecter les failles tels des audits d'applications Web, des audits de code et des tests d'intrusion entre autres.