



Interviews

Vincent Bieri, premier prix de l'innovation technologique, Monaco, octobre 2006

Par Isabelle Tisserand, coordinatrice du Cercle Européen de la Sécurité des Systèmes d'Information

Actualités

>Articles

>Veilles

>Comptes-rendus

Agenda

Annuaire

Infos Cercle

Parrainage

Archives

Votre avis nous intéresse...

Contacts

Les Assises

L'Exclusiv

Mentions légales

Vie privée

Se déconnecter

Comment est né ce projet ?

Du point de vue technologique c'est Pedro Bados, actuel CTO de NEXThink qui fut l'initiateur de ce projet en déposant un premier brevet sur les travaux de recherche qu'il menait à l'époque au Laboratoire d'Intelligence Artificielle (LIA) de l'EPFL (Ecole Polytechnique Fédérale de Lausanne) Ce brevet intitulé "Method of detecting anomalous behaviour in a computer network" est à la base de la technologie qui est implantée aujourd'hui au cœur du produit REFLEX de NEXThink. La mise en route de la société NEXThink et de ses premiers succès commerciaux ont été le fruit de la rencontre de quelques personnes qui pouvaient conjointement réunir les compétences et l'expérience nécessaires à la gestion et la croissance d'une entreprise comme à la connaissance approfondie du marché et des besoins en sécurité des systèmes d'information (plus d'informations sur : www.nextthink.com/team.html)

De part nos très bons contacts commerciaux acquis dans nos activités passées, les premiers prototypes disponibles du produit ont pu être mis à l'épreuve au sein d'environnements de production réels dans des sociétés qui sont aujourd'hui nos clients. Cette interaction permanente avec la réalité du terrain lors de la phase de développement initiale nous a permis d'avancer rapidement vers les besoins prioritaires des utilisateurs et d'assurer la qualité du logiciel et de celle de sa mise en œuvre. Nous avons annoncé la disponibilité de la première version commerciale de REFLEX après à peine un an d'existence, soit en septembre 2005 ; version immédiatement commandée par notre premier client pour un environnement multi-sites de plus de 6000 utilisateurs.

Ce qui a motivé mon choix de me lancer dans cette aventure, c'est à la fois la volonté d'entreprendre un projet ambitieux comme le sentiment que l'embryon de technologie découvert à l'EPFL pouvait entrevoir l'espoir d'arriver à offrir enfin une solution, cette pièce manquante du puzzle des besoins en sécurité qu'est la gestion du facteur humain. Mais, par-dessous, c'est de toute façon une affaire d'hommes qui, ensemble, se voient capables de réussir. C'est donc cette réunion d'une technologie nouvelle, d'un besoin du marché et d'hommes de valeurs et de qualité qui m'ont motivé à partir dans cette aventure et à apporter toute mon expérience acquise, entre-autres, comme responsable du marketing pour l'Europe des offres sécurité d'une grande société américaine (Cisco)

Combien de temps avez-vous consacré à son développement ?

Pedro Bados a mené ses recherches en intelligence artificielle pendant plus de deux ans puis, avec l'équipe fondatrice de la société, nous avons développé la solution pendant un an avant la disponibilité de la première version commerciale. Les premiers succès commerciaux comme la première levée de fond auprès de venture capitalist nous ont permis d'étoffer l'équipe pour poursuivre plus activement le développement de nos technologies et d'offrir une solution toujours plus

complète et plus efficace pour nos clients. Aujourd'hui près de 20 personnes travaillent pour NEXThink.

Le produit s'adresse t-il autant aux entreprises privées que d'Etat ?

Tout à fait. La problématique de la gestion du facteur humain concerne tous les types d'environnements. Nous avons des clients dans les divers secteurs privés comme ceux des administrations publiques. La taille des entreprises est fortement variable avec des petites institutions financières d'une centaine de personnes comme des industries ou des administrations de milliers ou même dizaines de milliers d'utilisateurs.

Après les investissements importants réalisés par les entreprises pour protéger leurs périmètres, les cabinets d'analyses insistent désormais sur la nécessité de sécuriser les serveurs et les postes de travail sur les réseaux internes (cf. «Protecting the Evil Insider» Burton Group, Novembre 2005) En effet, 75% des pertes déclarées par les entreprises proviennent de l'interne alors que respectivement 97%, 96% et 72% des entreprises concernées utilisent des pare-feux, anti-virus et IDS (cf. CSI/FBI Survey 2005)

Si les solutions traditionnelles semblent peu adaptées, c'est sans doute parce qu'elles sont orientées principalement sur la défense des périmètres et ne prennent pas assez en compte les nouvelles menaces discrètes exploitant souvent les failles comportementales du couple homme-machine.

La question prédominante concernant la sécurité interne serait donc plutôt : "l'activité des utilisateurs et des applications présente-elle un danger pour la sécurité de l'entreprise? Si oui dans quelle mesure et comment réagir rapidement?" La solution REFLEX de NEXThink permet de répondre à ces questions en offrant d'améliorer la sécurité interne des entreprises (en particulier les problèmes liés au facteur humain)

REFLEX permet de découvrir anonymement le comportement de la totalité des applications utilisées au niveau des postes de travail et des serveurs.

REFLEX permet de comprendre l'usage des applications par les utilisateurs et donc d'identifier : l'impact des problèmes potentiels liés à l'usage anormal, suspect ou illégal des applications, la perception des risques par les utilisateurs, le respect de la Charte d'utilisation et d'adapter les préconisations pour améliorer les programmes d'information et de sensibilisation. REFLEX permet également d'analyser très rapidement le comportement anormal ou atypique des applications et des utilisateurs et donc de valider : l'alignement de la politique de sécurité avec les menaces réelles avec une analyse des risques en la basant sur les comportements réels des applications et des utilisateurs, la configuration et l'efficacité des équipements de sécurité, la réactivité suite aux incidents liés à des anomalies d'utilisation des applications.

Au-delà de la solution REFLEX, NEXThink a mis au point une suite de méthodologies qui permettent de tirer un profit maximum de la technologie REFLEX. NEXThink et les méthodes EBA (Endpoint Behavior Assessment), SPA (Security Policy Audit) et MAP (Management of Awareness Program) qui s'articulent autour de la solution REFLEX et permettent de manière efficace et mesurable la construction et la gestion du risque et des anomalies.

Quelles sont les infrastructures techniques nécessaires à son fonctionnement ?

Les objectifs fixés :

- **Facile à déployer** dans un environnement opérationnel. La solution peut être installée quasiment instantanément de manière indépendante de l'infrastructure informatique. Le déploiement opérationnel est une question de jours.
- **Facile à maintenir** et sans besoin de configuration. La solution est capable de détecter et d'identifier toutes les applications commerciales ou développées "maison" (à façon)
- **Non intrusive** pour les utilisateurs qui ne perçoivent aucun impact sur le fonctionnement ou la performance de leurs outils informatiques.
- **Puissante** : les informations traditionnellement invisibles pour les autres systèmes car cryptées par l'utilisation de réseaux virtuels privés sont accessibles.
- **Intuitive** grâce aux techniques de visualisation de l'information avancées brevetées.

Les bénéfices recherchés :

- Protéger des menaces inconnues : non seulement en détectant en temps réel les applications non-conformes et les nouvelles menaces (attaques menées sur des utilisateurs spécifiques et abus internes) mais aussi en fournissant les moyens de surveillance en continu.
- Intégrer la dimension humaine avec l'évaluation des utilisateurs et de leurs comportements, de façon unitaire et/ou par groupes.
- Réduire la complexité et donc les coûts opérationnels en réduisant de manière drastique le temps pour comprendre et réagir aux problèmes par des outils de visualisation innovants.
- Permettre de se conformer aux nouvelles réglementations internationales en termes de pratiques, d'audit et d'administration de l'informatique et de l'entreprise en général.
- Permettre le stockage en ligne des données pour investigation sur une longue période d'activité pour des milliers de postes de travail connectés.
- Protéger les investissements déjà effectués en permettant une intégration de nos solutions à l'existant.

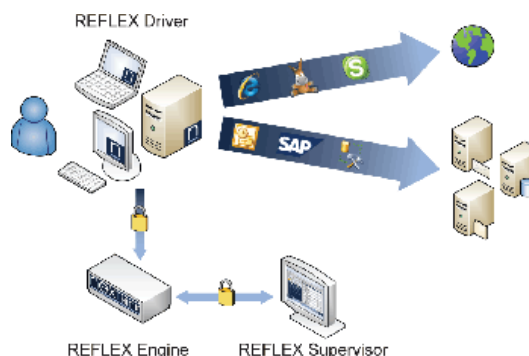
L'architecture :

REFLEX est composé de 3 composants

REFLEX driver

REFLEX Engine

REFLEX Supervisor



Les **REFLEX drivers** fonctionnent de manière passive sur les points terminaux (ordinateurs portables, stations de travail, serveurs, etc.) et capturent en temps réel des empreintes d'activités de toutes les applications et de leurs contextes. Exemples : qui utilise telle application ?, vers quelle machine ? Et comment elle communique (adresses IP et ports) ?

- Driver très léger (15Ko) sans impact sur les performances du poste de travail ou du temps de réponse des applications
- Contrôle des fichiers binaires liés aux applications (hash et version)
- Couches multiples de protection du driver
- Communication sécurisée vers le moteur d'analyse (REFLEX Engine)

Le **REFLEX Engine** collecte les informations des REFLEX drivers, modélise les comportements, analyse et détecte instantanément tous les changements tout en fournissant les capacités de stockage, de recherche rapide et de surveillance

active. Plusieurs REFLEX Engines peuvent être déployés : techniques de datamining et d'agrégation visant à réduire le trafic, analyse de type « Bayésien Network » pour l'évaluation de l'activité anormale, modèle « Hidden Markov Chain » pour la détection des évidences d'activités atypiques, techniques de type « Pattern Matching » pour les groupes de connexions atypiques, base de données performante embarquée avec des capacités de stockage local importantes.

Le **REFLEX Supervisor** est l'interface utilisateur pour comprendre, réagir, analyser et valider. Plusieurs REFLEX Supervisor peuvent être installés et les accès simultanés vers le même REFLEX Engine sont possibles.

Graphiques 2D est utilisé pour la représentation des comportements d'un utilisateur particulier ou d'un groupe, d'une application ou d'un groupe. Visualisation dynamique pour les agrégations et représentation temporelle des alarmes, un moteur de recherche intelligent et flexible intégré pour faciliter les investigations et l'analyse.

Depuis combien de temps votre société existe-t-elle ?

La création de la société date de septembre 2004. L'historique est commenté dans votre première question. Son futur est peut-être tout aussi intéressant. Je me permets de donner quelques idées générales de ma vision. Focalisées initialement sur la sécurité dans les réseaux internes d'entreprise, les discussions en cours avec l'industrie des télécommunications montrent une possible application de la technologie REFLEX dans le domaine de la détection de fraudes, notamment pour le réseau mobile de 3ème génération (3G) Tout en ne perdant pas son focus initial, NEXThink compte évaluer les possibilités attractives dans ce domaine précis.

Revenons à vous, pouvez-vous nous parler de votre parcours professionnel ?

Diplômé en informatique de l'école d'Ingénieur de Fribourg, je dispose d'une solide expérience internationale de près de 10 ans dans les technologies de communication et de sécurité de l'information au sein principalement, de Cisco Systems. J'ai souvent l'occasion de prendre la parole lors de conférences traitant des domaines de la sécurité et j'ai aussi souvent été cité dans la presse. Dans ma fonction de CEO chez NEXThink, je suis responsable de la stratégie produit et commerciale et chargé de mener à bien la bonne marche de la société dans le but d'atteindre les objectifs fixés.

Pourquoi ces choix intellectuels et techniques ?

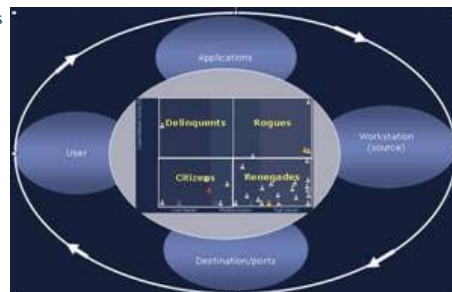
Nouvelles technologies, environnement informatique hétérogène, interactions complexes de logiciels, limites floues entre utilisateurs internes, mobiles ou ressources externes, expertise accrue des "hackers" sont quelques-uns des défis des organisations en charge de la sécurité. En dépit de nombreuses solutions telles que détection et protection contre les intrusions, pare-feu, anti-virus, tests de vulnérabilités et les promesses des constructeurs, un mécanisme infailliable de défense n'existe pas. Beaucoup de ces solutions sont très complexes à mettre en place et à maintenir, rajoutant de la complexité technologique au lieu d'en enlever. De plus, la plupart de ces solutions se concentrent sur la protection contre des menaces connues laissant les entreprises désarmées face aux nouvelles menaces non encore identifiées.

Pour lutter contre de telles menaces, NEXThink considère les utilisateurs et leurs comportements comme la pierre angulaire de son approche innovante. Le concept est simple : dans un réseau informatique, chaque utilisateur est nécessairement associé à une certaine identité électronique attachée à un comportement particulier et personnel. Chaque menace ou attaque est lancée, intentionnellement ou non, par un utilisateur spécifique, que cela soit un nouveau virus se propageant via le compte d'un utilisateur à son insu, un intrus utilisant un accès et un mot de passe subtilisés pour accéder aux systèmes internes ou un employé malveillant abusant de ses privilèges d'accès. En surveillant et en comprenant les changements de comportements des utilisateurs, NEXThink propose une dimension très intuitive et inexploitée pour découvrir les nouvelles attaques, évaluer les risques et déclencher les réponses ou les décisions appropriées.

NEXThink développe et commercialise une solution qui fournit une connaissance pertinente et en temps réel de l'activité des applications et des utilisateurs sur le réseau. Utilisateurs et applications sont automatiquement détectés et reconnus par le système, tous les changements significatifs de comportements sont immédiatement identifiés. Découvertes de nouvelles attaques, identifications immédiates de « spyware », utilisation d'applications non-conformes à la politique de sécurité sont seulement quelques exemples des capacités de la solution.

La solution de NEXThink s'appuie sur plusieurs innovations :

Modélisation du comportement des utilisateurs : basée sur des concepts d'intelligence artificielle, l'information traitée est modélisée dans un contexte intégrant la dimension "comportement humain" contrairement aux autres solutions qui ont plutôt tendance à ne considérer que des aspects techniques (séquences binaires, protocoles de communication) Ce modèle permet de déceler des comportements anormaux soit par rapport au comportement habituel d'un utilisateur soit par rapport à ceux d'autres groupes d'utilisateurs.



Prise d'empreinte d'activités en temps réel des comportements des applications réseaux : cette innovation permet de savoir de manière sûre et en temps réel d'où provient l'activité générée sur le réseau (utilisateur, application, machine, etc.)



Visualisation : généralement en sous-effectif, les administrateurs de sécurité sont confrontés à l'accumulation de tâches multiples, à la pénurie ou surabondance d'informations. NEXThink innove aussi dans les aspects de visualisation des informations et des problèmes afin d'extraire et de présenter l'information la plus pertinente. L'approche centrée sur les utilisateurs donne immédiatement accès à une dimension très intuitive plutôt que technologique.



L'innovation de la solution vient de son bénéfice immédiat en adressant un problème réel et actuel. Elle apporte une visibilité et une connaissance instantanée en temps réel et des capacités de détection et d'investigation historique des activités provenant de l'interaction entre utilisateurs et applications. La solution REFLEX de NEXThink est une pierre angulaire essentielle dans le cadre des méthodes EBA, SPA et MAP où REFLEX apporte la possibilité de réaliser un mapping avec la réalité lors des phases d'analyse de risques et de validation de politique de sécurité comme celles de mesures de retour sur investissement des programmes de formation et sensibilisation.



Quelles sont d'après vous et d'une manière générale, les attentes de vos clients en matière de sécurité ?

Après des années consacrées à la défense périmétrique, les analystes reconnaissent que la protection contre les menaces d'origine interne est devenue une priorité. Plus précisément, le débat actuel porte sur la faculté de découvrir l'usage réel des infrastructures et des applications et d'évaluer l'impact des vulnérabilités comportementales potentielles. A cet égard, les entreprises demandent de pouvoir réaliser des audits qui complètent les audits techniques traditionnels par l'analyse comportementale de l'usage des applications utilisant le réseau. Leurs objectifs sont d'obtenir une représentation dynamique de l'évolution de l'utilisation des applications et du comportement des utilisateurs et, en finalité, de capter de nouveaux indicateurs pour contrôler l'efficacité du Système de Management de la Sécurité de l'Information (SMSI)

Une demande en forte croissance est d'arriver à rendre plus efficaces les campagnes de sensibilisation destinées à élever le niveau de perception des risques par les utilisateurs, ce qui est finalement, le seul réel moyen de prévention efficace et adapté aux besoins d'agilité de l'entreprise. Autrement dit, tout bloquer n'est pas une alternative pour les entreprises même si en termes de sécurité cela serait une option à considérer. L'efficacité de ces campagnes est souvent remise en cause et aucune possibilité de mesure n'est généralement prévue à leur lancement. La bonne gestion de ces programmes passe par une segmentation réaliste des utilisateurs basée sur une analyse comportementale préalable. Les utilisateurs peuvent être ainsi regroupés en fonction de leurs usages des applications, et bénéficier ainsi d'un message adapté avec un impact plus fort. La mise en place d'un nouveau tableau de bord pour assurer la gestion des campagnes de sensibilisation et en mesurer l'efficacité est utilisée comme une empreinte de départ. L'utilisation continue pendant et après la campagne permet de mesurer objectivement si le niveau de perception des risques s'est amélioré ou non.

Pensez-vous que nous soyons à l'aube de grandes découvertes en matière d'innovations technologiques ?

Il existe de nombreuses innovations chaque jour et le rythme ne cesse de s'accélérer car chaque découverte sert à développer la suivante plus rapidement, et ceci dans tous les domaines technologiques. En ce qui concerne la sécurité je pense que nous allons assister à une convergence des technologies et à l'adoption de technologies collaboratives.

Qu'aimeriez-vous changer dans la galaxie des hautes technologies ?

Y apporter la dimension humaine trop souvent négligée et qui, si elle est bien gérée, apporte toujours un meilleur retour sur investissement technologique. L'objectif initial est souvent manqué non pas parce que la technologie utilisée est intrinsèquement inefficace mais parce que son intégration dans la chaîne d'utilisation et de gestion le devient. Soit qu'il devient humainement impossible d'exploiter efficacement une technologie (gestion optimale et coûts) soit que l'impact du facteur humain fait dévier les objectifs initiaux (erreurs, malveillance). Si je reviens sur la sécurité de l'information, les exemples sont nombreux. La gestion efficace des logs malgré les progrès technologiques (algorithmes de corrélation, formats standards) n'est toujours pas réellement une réalité et ne permet clairement pas d'atteindre les objectifs initialement fixés. Les technologies de prévention permettent efficacement de défendre les périmètres mais, malgré les promesses, restent quasi inefficaces en interne car c'est plus la notion de "human firewall" qui est essentielle et qui n'est pas du tout gérée efficacement par uniquement la technologie. Quels que soit les progrès technologiques, l'attitude de l'entreprise et de son personnel est ce qu'il y a de plus important car on ne peut pas protéger des données importantes avec la simple technologie, aussi avant-gardiste soit-elle. Il faut donc innover et créer des solutions qui permettent d'offrir des solutions efficaces à des besoins mais ces solutions se doivent d'intégrer une composante humaine pour devenir réellement exploitables jusqu'au bout et sans failles, simplement liées au comportement humain associé à son utilisation.

Quel conseil majeur donneriez-vous, en 2007, à tous les professionnels de la sécurité des systèmes d'information ?

Une compagnie peut mettre en application les meilleures technologies de sécurité disponibles, mais si l'impact du facteur humain ne fait pas partie intégrante des procédures de sécurité et de la gestion des risques, l'information et l'organisation sont et restent toujours dangereusement vulnérables. Développer une solution complète de sécurité se doit d'inclure les menaces de sécurité de l'information qui viennent de l'intérieur de l'organisation en intégrant une réelle capacité de diagnostic permanent des risques et de réactivité face aux incidents couplé à un programme efficace de sensibilisation des employés.

Quels sont vos futurs projets ?

Actuellement, sur le plan professionnel, je suis entièrement dévoué à ce que notre innovation se transforme en pleine satisfaction pour nos clients d'aujourd'hui et de demain. Les retours sont excellents mais il nous reste encore du chemin à faire et je sais que ce chemin sera rempli de nouveau projets que je me réjouis déjà de voir naître et qui, je l'espère, donneront satisfaction à nos clients. Nous continuons à faire de la recherche en partenariat avec plusieurs universités telle que l'Ecole Polytechnique où REFLEX a vu le jour. Ces travaux menés aujourd'hui sont clairement les embryons de solutions que nous offrirons demain. Ce ne sont donc pas les projets qui manquent dans le domaine des technologies de visualisations où nous sommes déjà très à la pointe. Mais nous pensons que nous pouvons encore faire plus. Les technologies mobiles ou des solutions flexibles, efficaces, mais aussi légères, doivent voir le jour compte tenu de la croissance des risques liés à l'explosion des systèmes mobiles pour non seulement la voix mais aussi les données qui sont maintenant utilisées dans les entreprises et par les gouvernements. Dans ce domaine, les vulnérabilités comportementales sont tout aussi cruciales que celles du réseau traditionnel.

Merci Vincent. Que 2007 vous apporte toute l'énergie nécessaire à votre créativité.