ipls

Suite tbt/400

PROGICIELS D'EXPLOITATION DES COMMUNICATIONS SUR **IBM iSeries-AS/400**

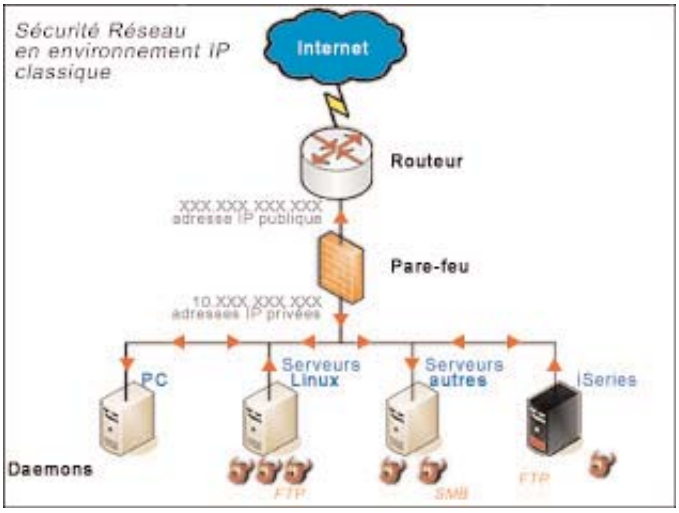
TBT400 COMMUNICATION iSeries

Sécurité Réseaux Externes

Comment s'intègre l'échange de fichiers automatisé dans une architecture déjà sécurisée sans introduire de faille de sécurité supplémentaire ?

Le risque est dans la portée de ce que sait faire l'application, d'où l'utilité d'un progiciel de communication comme TBT/400 qui apporte une aide colossale dans la gestion de ces risques par :

- **une sécurité générale d'implémentation**
- **une protection contre l'usurpation d'identité**



Ces clients qui nous font confiance :

- LES FORGES DE BOLOGNE
- WESTAFLEX
- EUGENE PERMA France
- POMONA
- SYSTEME U
- VETO SANTE
- CREDIT MUNICIPAL
- COGESAL - MIKO
- MARK IV - SYSTEMES MOTEURS
- EXIDE BATTERIES Ltd
- HUTCHINSON
- THYSSENKRUPP España
- ...

Sécurité générale d'implémentation

- **signature TBT**
  TBT400 utilise la signature TBT et non celle de l'OS400 puisque tous ses logins et passwords lui sont propres. TBT n'introduit donc **aucune nouvelle faille de sécurité** sur votre système, de cette façon, vous êtes sûr que toute usurpation d'identité effectuée à son niveau ne mettra jamais en péril votre iSeries-AS/400.

- **création dynamique des fichiers reçus**
  TBT400 crée et nomme toujours dynamiquement les fichiers reçus et ce quelque soit le nom réseau que lui donne l'utilisateur. Deux transferts ne peuvent donc en aucun cas s'écraser mutuellement.
  Il est impossible de prédire (de l'extérieur) le nom et l'emplacement d'un fichier dans TBT. Par ailleurs, ne sont visibles de l'extérieur que les fichiers mis à disposition de façon explicite et utilisant des noms toujours différents de leur nom réel.

Ces deux principes de base de TBT400 dispensent l'exploitation de toute notion de sécurité objet sur le iSeries-AS/400.

- **aucune arborescence de fichiers exposée**

- **rejet systématique des Remote commandes**
  TBT400 garde ainsi la main sur tous les fichiers interdisant de fait à un éventuel correspondant de prendre le contrôle de la machine.

- **pas de partage de fichiers**
  ceci permet de vous affranchir de ce qu'il convient d'appeler " une faille béante " si elle n'est pas accompagnée par la mise en place d'une véritable gestion de la sécurité objet. Il est à noter que **la sécurité objet est de la responsabilité de l'exploitation** (et non du réseau), de plus, elle implique une mise en œuvre particulièrement lourde et un audit régulier.

- **traitement au fil de l'eau**
  avec TBT400, le traitement des fichiers en réception est évènementiel. Cela dispense d'inventer une logique de synchronisation entre l'émetteur et le récepteur ; à savoir qu'il n'est donc nullement nécessaire de définir un "sur-protocole" d'échange avec les correspondants. Seuls les fichiers complets partent en traitement.
  Cette logique permet à n'importe quel Client ou Serveur distant de s'intégrer dans l'exploitation sans développer de logique particulière.

Protection contre l'usurpation d'identité

- **support de SSL et des certificats X.509**
  TBT400 gère le cryptage SSL et permet des **échanges cryptés** dès lors que le correspondant supporte le SSL. Ceci rend très difficile une écoute du trafic.

- **le contrôle d'adresse natif** dans TBT permet de protéger efficacement les correspondants disposant d'une adresse IP fixe.
  En d'autres termes, ceci permet de contrôler de façon strict l'adresse de l'appellant, ainsi, même si un utilisateur non autorisé arrive à se procurer un mot de passe valide, encore faudra t-il qu'il se connecte à partir d'une adresse autorisée.

- **la lecture destructive** autorise une seule lecture pour un fichier donné. De plus, elle n'est possible que pour les éléments explicitement mis à disposition et protège de fait contre les dangers du partage de fichiers.
  Chaque fichier traité est retiré de la liste des fichiers disponibles. Cette méthode permet de limiter les risques encourus en cas d'usurpation d'identité. Un individu non autorisé ne pourra pas lire un message déjà lu puisqu'il ne sera tout simplement plus " visible ". Par contre, si ce même individu arrive (en étant le premier à se connecter) à récupérer le fichier, il y aura effectivement accès mais l'utilisateur légitime en sera rapidement informé puisque lui-même ne pourra plus y accéder. TBT ne peut donc pas empêcher l'usurpation d'identité mais, en vous permettant de la déceler très rapidement, il participe à rendre votre système encore plus sûr.

- **les utilisateurs sont nativement isolés entre eux**

les points ci-dessus ont pour fonction de minimiser l'impact d'une usurpation d'identité tout en permettant l'alerte en cas d'usurpation d'identité.

La sécurité TBT400 ne permet aucune ouverture sur la sécurité du 400 : AUCUNE FAILLE SUPPLEMENTAIRE A VOTRE EXISTANT

Quelques définitions

- **Usurpation d'identité**
  Cas de figure lorsqu'une personne non autorisée arrive à se procurer les "login & password" d'un utilisateur légitime et à en faire usage au sein d'un système informatique. Il s'agit d'un risque de sécurité particulièrement élevé contre lequel il est très difficile, voir impossible, de se prémunir.

- **Remote Commands**
  Commandes spécifiques à l'iSeries-AS/400 qui permettent à un utilisateur d'exécuter du code sur une machine distante. Bien que très pratiques ces commandes entraînent un risque de sécurité évident qu'il convient de maîtriser.

- **Ecoute du trafic**
  Méthode utilisée par de nombreux pirates qui consiste à récupérer des informations circulant en clair sur le réseau. Un protocole comme FTP n'implémente pas le cryptage des données, il est donc possible, par cette méthode, de récupérer des informations aussi sensibles que les "passwords" utilisateur.

- **Sécurité Objet**
  Fonctionnalité de l'iSeries-AS/400 qui permet de contrôler très précisément chacun des objets du système (se compte en dizaine de milliers). Il est ainsi possible de mettre en place une politique de sécurité très strict et particulièrement efficace. En contre partie, et c'est ce qui la rend si "impopulaire", elle implique une mise en œuvre très lourde et des audits quotidiens du fait, par exemple, de la possibilité de créer des objets dynamiquement.

- **Partage de fichiers**
  Permet de mettre facilement à disposition de plusieurs utilisateurs le contenu d'un répertoire. L'ouverture du partage de fichiers sur un répertoire de l'iSeries-AS/400 le rend implicitement disponible à tous les utilisateurs de toutes les machines du réseau. Garantir la sécurité d'un tel système c'est mettre en place une véritable sécurité objet et/ou le développement d'exit de contrôle.

La sécurité peut être encore renforcée dans le cadre de l'utilisation de multiTBT associé à une DMZ.

IPLS
176, Bureaux de la Colline
92210 Saint-Cloud
FRANCE
Tél. +33 (0)1 80 41 00 60

Email : ipls@ipls.fr
Sites internet :
http://www.ipls.fr
http://www.tbt400.com

Notre Partenaire :