Technologies informatiques appliquées au commerce électronique

Travail d'études de Simeon Kostov et Dimitre Kostov

Licence Informatique 2002-2003

Université de Nice

« Internet sera à l'économie du 21ème siècle ce que l'essence fut au 20ème siècle »

Craig Barret - PDG d'Intel

1. Introduction

Le but de notre travail d'études et d'explorer les infrastructures et les technologies informatiques utilisés dans un des domaines les plus dynamiques de notre actualité - le commerce électronique. Malheureusement on a constaté que la plupart des informations disponibles sur ce sujet étaient soit sous la forme « Comment construire un site e-commerce et gagner beaucoup d'argent (en 500 pages) », ce qui est d'après nous un gaspillage de ressources et de papier, soit plutôt spécialisées du côté marketing et gestion, ce qui ne nous intéresse pas beaucoup. On a essayé d'écrire un rapport bref, synthétique et accessible à un large public, au lieu de faire un rapport long contenant des informations lourdes et inutiles.

2. Définition et Histoire

Qu'est-ce que c'est que le commerce électronique? A cette question la plupart des gens évoquent l'image des sites Web biens connu comme fnac.fr, amazon.com, etc. qui leur permettent de commander des différentes marchandises, payer en ligne par carte bancaire et ensuite être livré par la poste. Mais la réponse de cette question n'est pas si simple, on peut parler de commerce électronique quand on paie des impôts en

ligne, quand on retire de l'argent à partir d'un DAB, ou même quand on utilise le téléphone pour consulter les résultats du loto (une service qui est facturé plus cher qu'une communication normale). On va définir le e-commerce comme une **échange des informations** commerciales sur un **réseau** composé d'appareils électroniques (normalement des ordinateurs).

Avant l'invention de l'ordinateur, les premières formes de commerce électronique consistaient en passer des ordres commerciaux à distance, par le télégraphe et plus tard par le téléphone.

Vers la fin des années 60 le système EFT (Electronic Funds Transfer) est mis en place aux Etats-Unis, en permettant le transfert électronique de fonds entre banques (à travers des réseaux privés et sécurisés).

Au début des années 70 la technologie EDI (Electronic Data Interchage) a été développée. Standardisée plus tard par les normes ANSI X-12 et UN/EDIFACT, EDI est un ensemble de normes utilisées pour l'échange de l'information (normalement des documents commerciaux) entre les ordinateurs et pour le traitement électronique des transactions commerciales.

En 1982 France Telecom commercialise le minitel - un système qui trouve vite des applications dans la vente par correspondance. Le minitel est un terminal "mort", c'est-à-dire qu'il s'agit uniquement d'un clavier et d'un écran, sans processeur ni dispositif de stockage. Les services sont accessibles depuis une ligne de téléphone grâce au modem incorporé.

Le "grand boom" du commerce électronique (1995-97) est venu de l'expansion de l'Internet: aux Etats-Unis, les grandes entreprises comme les plus petites ont, à partir de leurs sites Web, ont réussi à approcher les consommateurs "en temps réel" et à leur proposer des catalogues en ligne, des moyens de commandes et de paiements, mais aussi des prix attractifs (notamment grâce aux économies réalisées sur le stockage et les intermédiaires).

Aujourd'hui nous sommes témoins d'une autre expansion du commerce électronique, le commerce B2B (les échanges entre entreprises) qui est cette fois-ci internationale au lieu d'être centrée sur les marchés domestiques.

3. Structure informatique d'un commerce sur Internet

La structure informatique d'un commerce en ligne est généralement divisée en deux parties :

- le « front office », ou boutique
- le « back office », ou outil de gestion

Le back-office est parfois fusionné avec le front office dans les cas les plus simples.

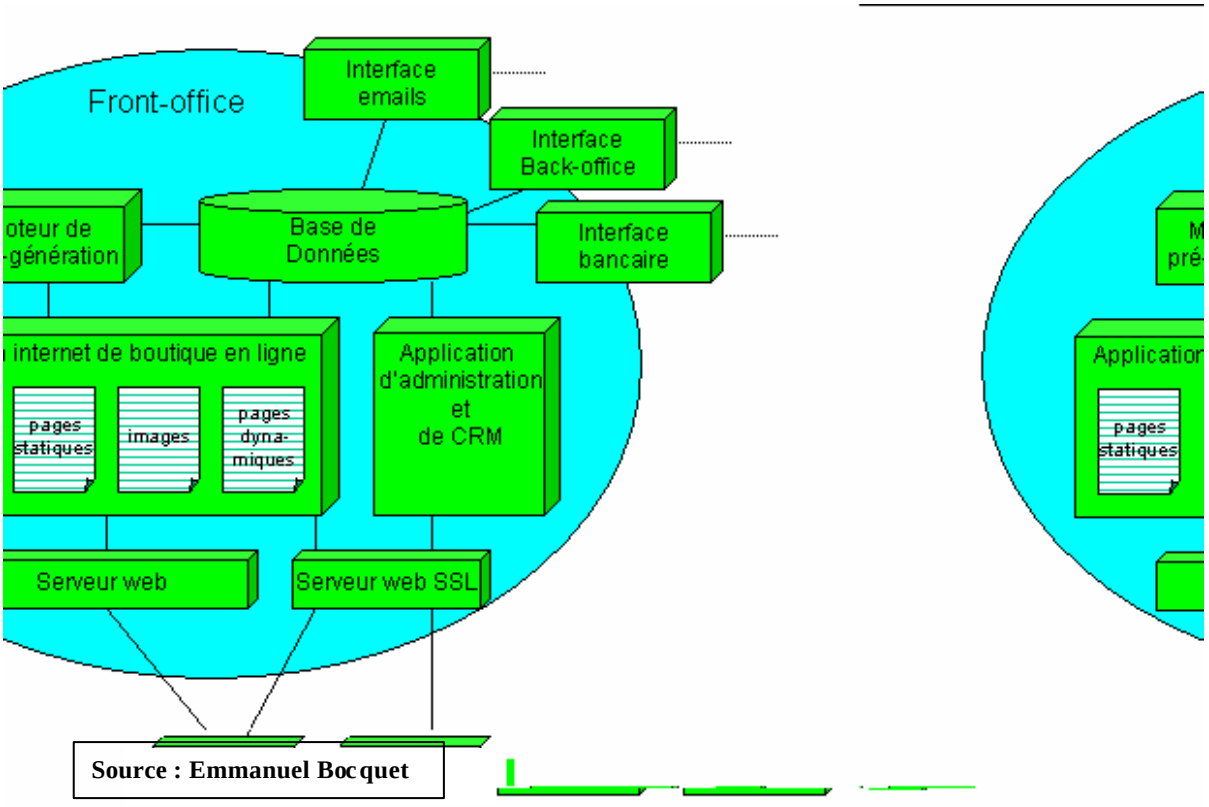
3.1 Le front office

Le "front office" est le programme qui va interagir avec le client ou le prospect pour gérer la relation commerciale. C'est en quelque sorte la version Internet d'un magasin et

d'un vendeur. Typiquement, l'application se présente sous la forme d'un ensemble de pages Web, et se décompose en plusieurs modules :

- présentation de la société
- présentation de l'offre commerciale (catalogues)
- achat et paiement ("panier", commande, paiement sécurisé)
- gestion de compte client (adresses, abonnements)
- envoi et réception de mails (confirmation de commande)
- contenus éditoriaux (conseil, information, actualité)

Généralement, l'application du front office communique avec d'autres systèmes : la comptabilité, la logistique (achats, stocks, préparation de commande), l'administration du site.



3.2 Le back office

Un "back-office" combine l'ensemble de fonctions nécessaires à une boutique, exception faite de la partie commerciale. Il est constitué en particulier de logiciels pour :

- La gestion des achats et des fournisseurs
- L'administration des ventes et le suivi de commande
- La gestion de stock, d'entrepôt et la préparation de commande
- La comptabilité

Il existe de nombreux logiciels de gestion intégrés qui recoupent toutes ces fonctions, il y en a pour toutes les bourses et pour tous les métiers. La lourdeur de cette partie logicielle amène souvent les entreprises à opter pour des logiciels intégrés et livrés "clé en main" en sur-mesure par des éditeurs de logiciels reconnus pour diminuer les risques de dérapage. Au-delà de la dépendance que cela crée (et qu'il faut maîtriser sous peine de dérives), cela implique une souplesse encore diminuée ; en effet, toute modification du système pour améliorer son fonctionnement implique de faire appel à un éditeur ou à un prestataire spécialisé, dans des délais et des coûts souvent délicats. D'une manière générale, un back-office coûte rarement moins de 100.000 € et souvent plus de 300.000 €. Les logiciels back office les plus connus sont SAP, Oracle Application, Siebel et Business Objects.

4. La transaction électronique

Il existe plusieurs types de transactions électroniques, dans notre travail d'études on va nous concentrer sur le paiement par carte bancaire (les protocoles SSL et SET). Voici quelques types de transactions électroniques qu'on n'a pas abordé dans notre travail d'études:

- Transactions électroniques interbancaires(TARGET, SWIFT) - TARGET, acronyme de Trans-european Automated Real-time Gross settlement Express Transfers (Transferts express automatisés transeuropéens à règlement brut en temps réel) est le système à règlement brut en temps réel destiné aux paiements en euro.
- Micropaiements - pour les transactions d'un montant très petit (par exemple le coût d'un appel téléphonique, ou l'accès a une page Web payé)
- Argent électronique (eCash) - analogue électronique de l'argent liquide. On distingue deux formes d'argent électronique, selon le type de support électronique utilisé : l'argent stocké sur support matériel (carte à puce prépayée, tel le porte-monnaie électronique) et l'argent stocké sur support logiciel (disque dur, serveur bancaire, tel le porte-monnaie virtuel) facilement transférable par Internet. L'argent électronique est émis par une banque, et chacun des billets (ou chacune des pièces) comporte un numéro de série unique et représente une somme d'argent précise.

4.1 Le paiement par carte bancaire

Le paiement par carte bancaire sur Internet doit garantir à son propriétaire la confidentialité des données échangées, ainsi que minimiser, voire rendre impossible tout risque de fraude. Aujourd'hui deux protocoles sont utilisés – SSL, qui assure la confidentialité des données transmis par le Web et SET, qui est un protocole de paiement dans le sens propre du mot. Pour comprendre bien leur fonctionnement on d'abord expliquer la notion de certificats et autorité de certification.

4.1.1 Certificats et autorités de certification

Pour qu'un serveur puisse offrir le service de paiement sécurisé par carte bancaire il doit posséder une paire de clés - publique et privé et un certificat issu par une autorité de certification qui garantit la validité de sa clé publique. Un certificat numérique et une sorte de carte d'identité virtuelle, qui sert à identifier une personne, un service Web ou un serveur, ou plus précisément attester qu'une clé publique lui appartient bien. Pour cela il renferme des différentes informations - la clé publique bien sûr, le nom de la personne ou entreprise qui le détient, des dates de début et fin de validité, et d'autres informations supplémentaires. Pour garantir la conformité de ces données un certificat est issu par une autorité de certification (une sorte de préfecture virtuelle, par exemple CertiNomis, VeriSign) qui en signant numériquement le certificat avec sa clé privé atteste la validité des informations contenues. Il suffit alors a connaître la clé publique de cette autorité (largement distribué sur le Web, et parfois intègre dans des navigateurs comme dans le cas de VeriSign) pour décrypter cette signature numérique et ainsi vérifier la validité d'un certificat issu par elle.

4.1.2 Le Protocole SSL(Secure Socket Layer)

SSL est développé par Netscape en 1994 et représente un protocole Client / Serveur qui repose sur un protocole de transport tel que TCP/IP et assure une connexion privée et une authentification des extrémités. SSL n'est pas un protocole de paiement, mais il est largement utilisé dans le commerce électronique pour crypter le numéro de carte bancaire du client et le transférer au marchand. Une session SSL débute par le protocole de reconnaissance mutuelle (handshake) entre le client et le serveur, c'est-à-dire l'échange de messages entre les deux machines, donnant lieu à l'authentification. Le processus observe les étapes suivantes :

1. Le client établie une connexion au port sécurisé (une connexion « https »). Il expédie une requête, où il envoie sa version SSL et certaines autres données.

2. Lorsque le serveur reçoit cette information, il renvoie sa propre version SSL, ainsi que son certificat. Il peut également demander le certificat du client si l'authentification de celui-ci est requise.

3. Le client reçoit le certificat et vérifie sa validité, c'est-à-dire si le certificat est expiré ou non et s'il a été émis par une Autorité de certification de confiance. Les clients maintiennent une liste des certificats émis par les Autorités de certification reconnues, afin de déterminer la validité d'un certificat reçu.

4. Le client crée maintenant une clé secrète (« *premaster secret* »), qui sera utilisée dans cette session. Cette clé secrète est chiffrée à l'aide d'une clé publique trouvée sur le certificat du serveur, et envoyée ensuite à ce dernier.

5. Le serveur utilise sa clé privée pour décrypter la clé *premaster secret*, et crée ensuite une clé *master secret*, Le client crée lui aussi une clé *master secret*, à l'aide de la *premaster secret*.

6. La clé *master secret* est utilisé par le client et le serveur pour créer des clés de chiffrement et de décryptage de l'information, autant que pour détecter tout changement effectué par quiconque, pendant la transmission des données.

7. Le client informe le serveur qu'il a été lu, et qu'il va procéder au chiffrement des messages à l'aide de la clé de session. Le serveur envoie également un message similaire au client.

Une fois cela réalisé, toute donnée est chiffrée avant l'envoi, et décryptée avant d'être utilisée. L'intégrité des données est ainsi confirmée. Le succès de SSL s 'explique par sa simplicité d 'utilisation et par son intégration dans tous les navigateurs du marché.

4.1.2 Le Protocole SET (Secure Electronic Transaction)

SET est un protocole destiné spécialement à sécuriser les transactions Internet de paiement par carte bancaire. Il a été développé à l'origine par Visa International et Master Card, en 1996, avec l'aide des grandes compagnies informatiques de la planète. Son champ d'application se réduit au cryptage des seules données bancaires, contrairement à SSL qui peut chiffrer les images et le texte. Le protocole SET implique trois parties: le client, le vendeur et la banque du vendeur. Ce système SET requiert des certificats auprès des trois parties. Les certificats du client et du vendeur sont fournis par leur banque respective après quoi la transaction commerciale peut avoir lieu. Avec le SET, le numéro de carte bancaire ne peut pas être connu du vendeur, donc ne sera pas stocké dans ses fichiers et être récupéré par une personne mal intentionnée. Le SET assure en principe une transaction de non répudiation, mais cette clause peut varier d'un pays à l'autre suivant la législation en vigueur.
SET et extrêmement sûr – il permet une pleine identification réciproque des deux parties grâce à un tiers de confiance, en l'occurrence la banque du vendeur, mais à ce jour il est très peu utilisé. Une transaction SET nécessite aussi un logiciel spécial de côté client.

5. Les agents « intelligents » et leur rôle dans le commerce électronique

Un agent intelligent est d'après la définition de l'association française de normalisation (AFNOR) un "*Objet utilisant les techniques de l'intelligence artificielle : il adapte son comportement à son environnement et en mémorisant ses expériences, se comporte comme un sous-système capable d'apprentissage : il enrichit le système qui l'utilise en ajoutant, au cours du temps, des fonctions automatiques de traitement, de contrôle, de mémorisation ou de transfert d'information.* Il doit posséder les caractéristiques suivantes :

- Autonomie (indépendant de l'utilisateur)
- Capacité à communiquer et à coopérer avec d'autres agents

- Capacité à raisonner, à réagir à son environnement
- Mobilité. Les agents doivent pouvoir être multi-plate-forme et multi-architecture. Ils doivent pouvoir se déplacer sur le réseau où ils accomplissent des tâches sans que l'utilisateur ait le moindre contrôle sur celles-ci.
- Possibilité éventuelle de se reproduire

Quand on a plusieurs agents spécialisés qui collaborent entre eux, on parle d'un système « multi agent ». Applications : très variés – robotique, moteurs de recherche, notifications d'événements et bien sûr dans le commerce électronique.
On distingue deux catégories d'agents pour le commerce électronique : les agents acheteurs et les agents vendeurs.

5.1 Les agents acheteurs

Ils sont contrôlés par les clients et ont pour but de faciliter le processus d'achat. En effet, comme pour tout autre recherche, identifier et vérifier l'intérêt d'une offre commerciale est extrêmement difficile sur Internet si on utilise les outils classiques (moteurs et répertoires de recherche). Il est nécessaire d'identifier les sites Web marchands spécialisés, de déterminer si le produit recherché y est référencé, de prendre connaissance de son prix, et de répéter cette démarche sur tous les sites suivants. Les agents acheteurs sont capables de se connecter sur divers services de vente à distance et ramener les informations de description et de prix de tous les articles d'un type déterminé, pour en proposer la liste comparative, voire passer automatiquement la commande. Contrairement aux agents de recherche d'informations sur le Web, les agents acheteurs ne travaillent pas à partir de mots-clés mais à partir de noms de produits ou de marques. Ils renseignent l'utilisateur sur :

- la disponibilité d'un produit en menant une recherche par marque ou par catégorie
- l'identification des distributeurs: localisation d'un distributeur précis, liste intégrale ou sélective de distributeurs (en fonction des services qu'ils offrent: garantie, facilité de paiement, etc.).

Comme exemple on peut donner le site prixmateriel.com, qui permet à l'internaute de comparer les prix du matériel informatique auprès des différents marchands spécialisés.

5.1 Les agents vendeurs

Les différentes fonctions assurées par les agents vendeurs sont :

- Enregistrement du profil et des préférences de l'acheteur
- Enregistrement des demandes successives de l'acheteur afin d'enrichir, d'affiner, de faire évoluer son profil
- Aider à l'entreprise de comprendre le comportement des différents consommateurs

Les agents vendeurs présentent les biens et les services aux clients (qu'ils considèrent comme des agents) et peuvent même être programmés pour négocier, voire effectuer les transactions. Ce pourra être un billet d'avion, un rendez-vous. La transaction peut d'ailleurs se faire aussi bien dans l'autres sens. Les clients peuvent se faire enregistrer comme demandeurs d'un produit ou d'un service déterminé (par exemple la recherche d'un emploi). Un agent vendeur ayant un produit à commercialiser va traverser le réseau à la recherche des clients intéressés par ce produit. Lorsque l'agent vendeur rencontre un agent client intéressé par ce type de produits, une transaction est alors négociée entre les deux agents.

6. E-bibliographie

1. http://www.cyberfutur.qc.ca
2. http://membres.lycos.fr/bocquet/
3. http://www.rambit.qc.ca/plamondon/
4. http://www.finances.gouv.fr/cybercommerce/
5. http://www.planete-commerce.com/
6. http://www.agentintelligent.com/