Cours : Qualité des logiciels

Réalisé par : Mr Zakaria Taleb Essalama

Table des matières

I. Définitions

En informatique et en particulier en génie logiciel, la **qualité logicielle** est une appréciation globale d'un logiciel, basée sur de nombreux indicateurs.

La complétude des fonctionnalités, la précision des résultats, la fiabilité, la tolérance de pannes, la facilité et la flexibilité de son utilisation, la simplicité, l'extensibilité, la compatibilité et la portabilité, la facilité de correction et de transformation, la performance, la consistance et l'intégrité des informations qu'il contient sont tous des facteurs de qualité.

Un logiciel est un produit qui ne se détériore pas et qui est continuellement modifié. La qualité d'un logiciel dépend entièrement de sa construction, la qualité logicielle est par conséquence un sujet central en génie logiciel. Une appréciation globale de la qualité tient autant compte des facteurs extérieurs, directement observables par l'utilisateur, que des facteurs intérieurs, observables par les ingénieurs lors des revues de code ou des travaux de maintenance.

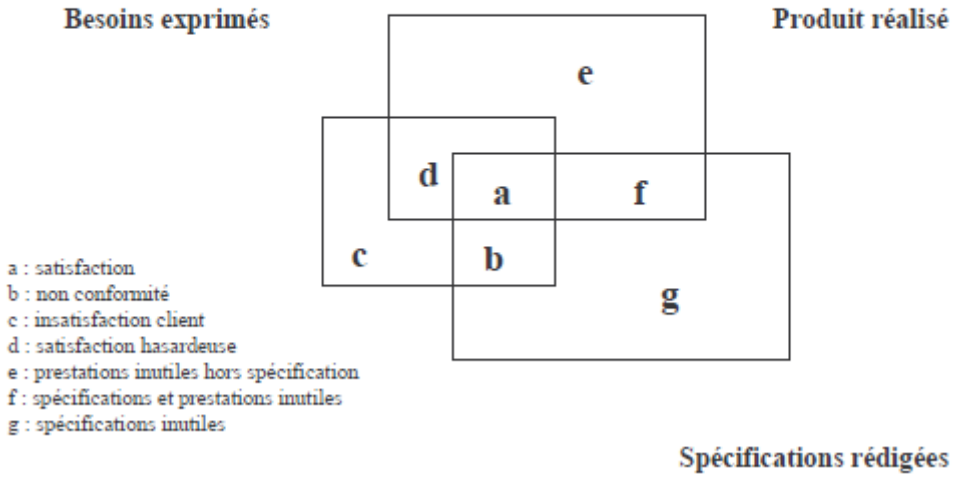
Les problèmes de qualité des logiciels, connus depuis les années 1960, sont par ailleurs à l'origine du génie logiciel : la science de la création de logiciels, y compris toutes les difficultés qui y sont liées - respects des coûts, des délais, du cahier des charges et du niveau de qualité.

Il existe un référentiel de certification du système de management de la qualité en entreprise, en matière d'ingénierie du logiciel le TickIT.

Facteurs de non qualité du logiciel

- Mauvaises spécifications
  - Vagues, incomplètes, instables
- Mauvaises estimations
  - Fausses, oublis, précisions insuffisantes
- Mauvaise répartition des tâches
  - Organisation inadaptée, contraintes omises
- Mauvais suivi
  - Ecarts non détectés à temps
- Mauvaise réalisation technique
  - Codage, tests, documentation
- Problèmes humains
  - Mauvaise distribution des travaux
  - Conflits, rétention d'information
- Manque d'expérience du métier de Chef de projet

Le problème de la conformité aux besoins



II. Indicateurs de qualité logicielle

La norme ISO 9126 définit six groupes d'indicateurs de qualité des logiciels:

1. la capacité fonctionnelle. c'est-à-dire la capacité qu'ont les fonctionnalités d'un logiciel à répondre aux exigences et besoins explicites ou implicites des usagers. En font partie la précision, l'interopérabilité, la conformité aux normes et la sécurité
2. la facilité d'utilisation, qui porte sur l'effort (le peu d') nécessaire pour apprendre à manipuler le logiciel. En font partie la facilité de compréhension, d'apprentissage et d'exploitation et la robustesse - une utilisation incorrecte n'entraîne pas de dysfonctionnement
3. la fiabilité, c'est-à-dire la capacité d'un logiciel de rendre des résultats corrects quelles que soient les conditions d'exploitation. En font partie la tolérance de pannes - la capacité d'un logiciel de fonctionner même en étant handicapé par la panne d'un composant (logiciel ou matériel) ;
4. la performance, c'est-à-dire le rapport entre la quantité de ressources utilisées (moyens matériels, temps, personnel), et la quantité de résultats délivrés. En font partie le temps de réponse, le débit et l'extensibilité - capacité à maintenir la performance même en cas d'utilisation intensive ;
5. la maintenabilité, qui porte sur l'effort (le peu d') nécessaire en vue de corriger ou de transformer le logiciel. En font partie l'extensibilité, c'est-à-dire le peu d'effort nécessaire pour y ajouter de nouvelles fonctions ;
6. la portabilité, c'est-à-dire l'aptitude d'un logiciel de fonctionner dans un environnement matériel ou logiciel différent de son environnement initial. En font partie la facilité d'installation et de configuration pour le nouvel environnement.

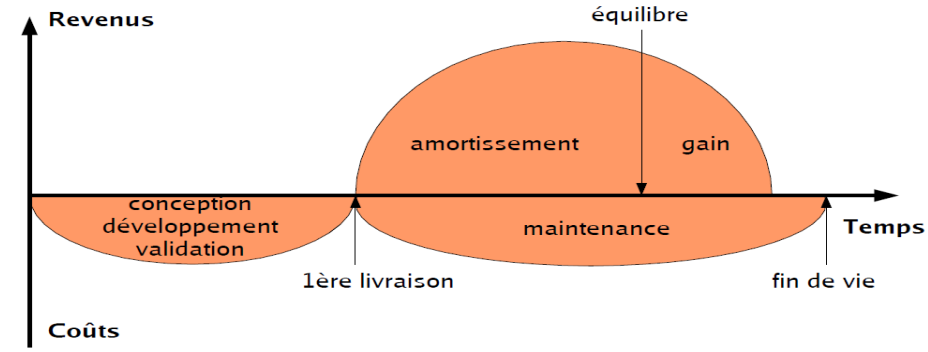
Chaque caractéristique contient des sous-caractéristiques. Il y a 27 souscaractéristiques.

III. Cycle de vie

Ensemble séquentiel de phases, dont le nom et le nombre sont déterminés en fonction des besoins du projet, permettant généralement le développement d'un service ou d'un produit

1. Vie d'un logiciel

(d'après J. Printz)



2. Quand un logiciel est-il terminé ?

- quand on a fini de le programmer ?
- quand on l'a compilé ?
- quand il s'exécute sans se planter ?
- quand on l'a testé ?
- quand on l'a documenté ?
- quand il est livré au premier client ?
- quand il n'évolue plus ?
- quand il n'est plus maintenu ?

3. Pourquoi se préoccuper d'un « cycle de vie » ?

C'est un processus

– phases : création, distribution, disparition

● But du découpage

– maîtrise des risques

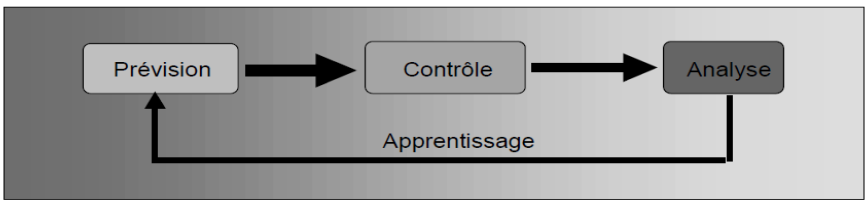
– maîtrise des délais et des coûts

– contrôle que la qualité est conforme aux exigences (→)

● En fait, problématique plus générale

– mais spécificités relatives aux logiciels

Processus



4. Les phases d'un cycle de vie
   1) Définition des besoins (cahier des charges)
   2) Analyse des besoins (spécification)
   3) Planification (gestion de projet)
   4) Conception
   5) Développement (codage, test, intégration)
   6) Validation
   7) Qualification (mise en situation)
   8) Distribution
   9) Support

a. Processus contractuels

Comment acquérir/développer un système sur mesure ?

– Que le logiciel soit

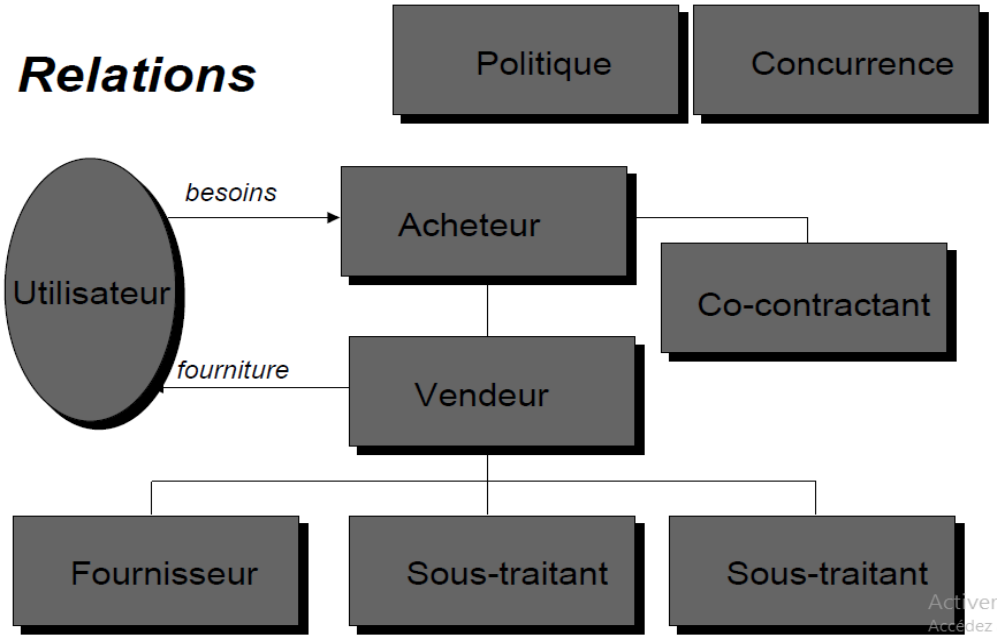
» développé en interne

» acheté, sous-traité

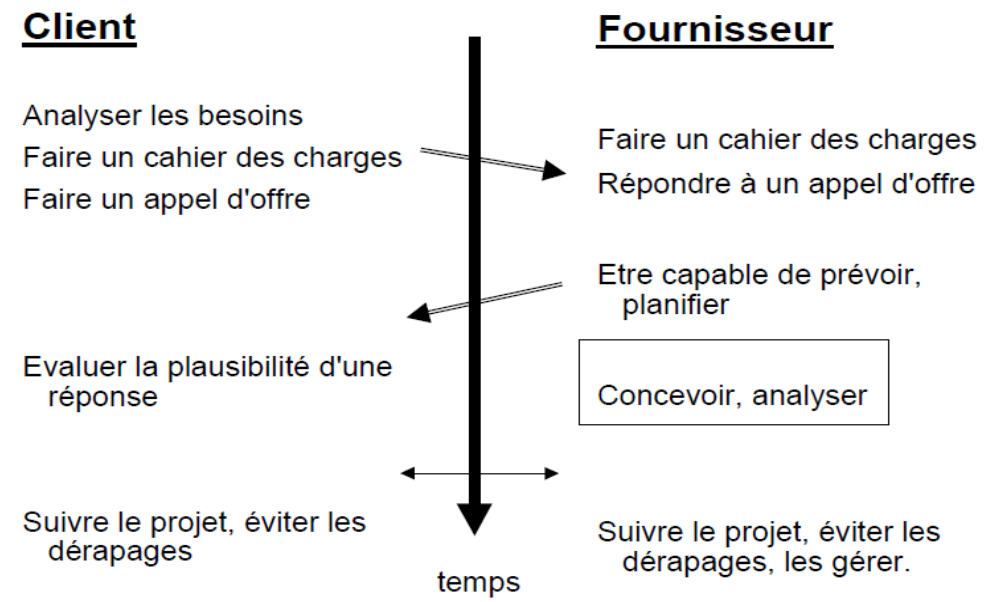
• Comment avoir/donner confiance

– respect des coûts, du calendrier

– respect des besoins fonctionnels



Points de vue



b. Exemple d'un cahier des charges de réalisation d'un site web

c. Analyse des besoins logiciels

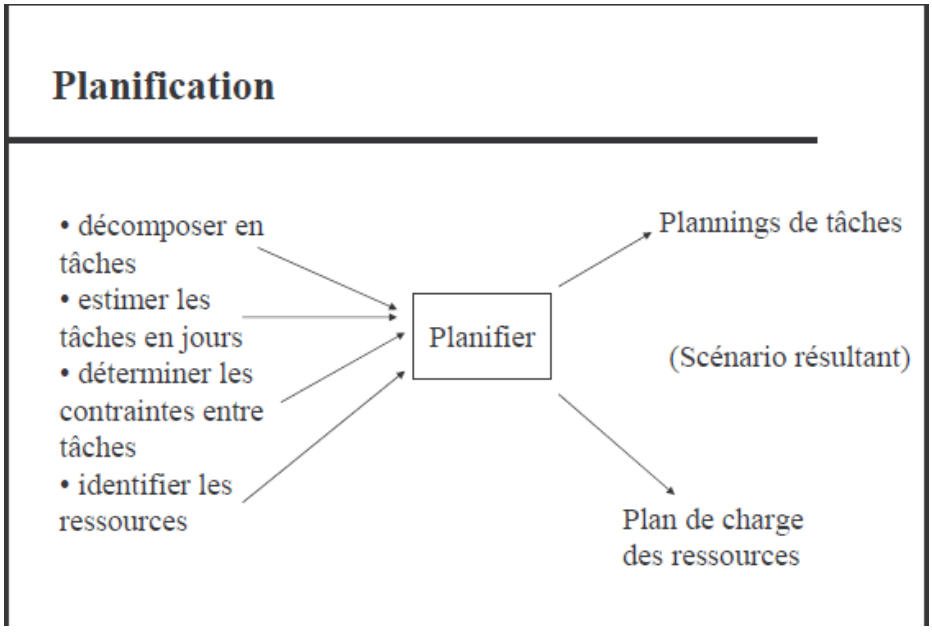
- Donner une modélisation du logiciel vu comme un système composé de sous-composants plus simples
- pour chaque sous-composant expliquer succinctement
  - ce qu'il fait
  - les entrées-sorties (fichiers, BD, signaux ...)
  - les principaux algorithmes
  - les performances attendues (ultérieurement tests)
- décrire les interactions entre les sous-composants
- préparer les tests de validation
- mise à jour de la planification du projet
- Dresser la liste des ressources existantes

(algorithmes connus, outils logiciels)

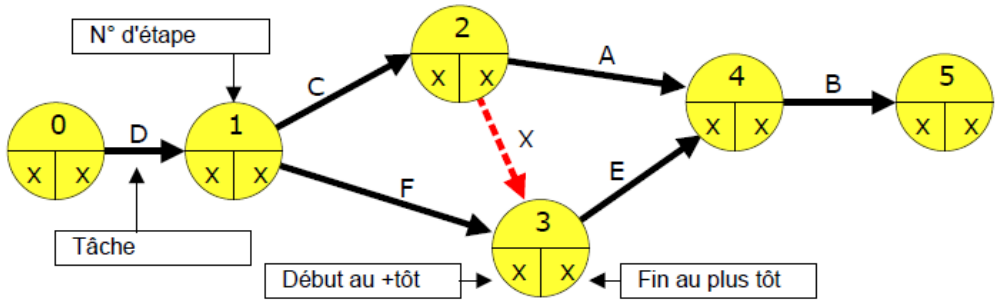
d. Planification

La planification permet de décrire l'enchaînement des différentes activités d'un projet. Elle s'appuie sur des estimations de durée ou d'effort associés à chacune de ces activités, puis décrit les dépendances entre les activités dans le temps.

A chacune des activités sont attribuées des ressources humaines, matérielles ou budgétaires. On peut ainsi avoir une vue globale dans le temps de la répartition :
· des efforts individuels - pour les ressources humaine,
· des dépenses et recettes - pour les ressources budgétaires,
· de l'utilisation des machines, instruments de mesure, etc. - pour les ressources matérielles.



e. Exemple de diagramme de pert



f. Processus de développement

Ce processus est une suite d'étapes pour le développement et la maintenance d'un système logiciel

- Spécification
- Conception
- Codage
- Validation
- Evolution

Le processus de développement industriel peut être décomposé en trois grandes activités :

Le processus technique : il modélise la procédure à suivre pour réaliser le produit.

Le processus de gestion : il modélise la procédure à suivre pour contrôler les délais et les coûts.

Le processus qualité : il modélise la procédure à suivre pour garantir la qualité du produit, des différents processus participant au développement du produit (gestion et qualité).

Chacun de ces processus peut lui-même être décomposé en trois grandes phases :

1. La prévision : consiste au début du processus à annoncer comment le processus se déroulera.

2. Le suivi et le contrôle : consiste au cours du processus à vérifier que ce qui se déroule est conforme à ce qui est annoncé ; sinon il faut, soit modifier les prévisions, soit agir sur le processus.

3. L'analyse : consiste à la fin du processus à revenir sur ce qui s'est passé pour apprendre et améliorer la prévision et le contrôle des futures réalisations (Feed-back).

7 bonnes pratiques pour le développement de logiciel :

- Développement à base de composants centré sur l'architecture
- Pilotage par les risques
- Gestion des exigences
- Maîtrise des modifications
- Evaluation continue de la qualité
- Modélisation visuelle

g. Processus d'exploitation et maintenance

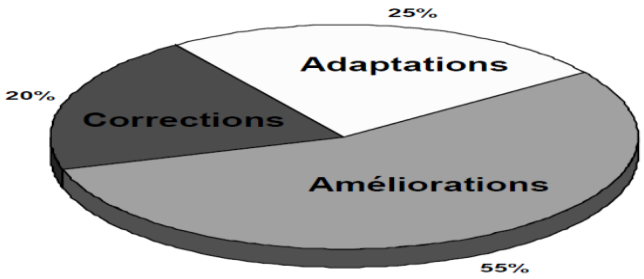
Cette étape correspond à l'exploitation du logiciel par tous les utilisateurs initialement envisagés. La maintenance consiste à modifier un programme après qu'il ait été livré.

Ces modifications peuvent consister à corriger des erreurs de codage, de conception ou de spécification.

Les modifications apportées par la maintenance peuvent également être réalisées pour prendre en compte une évolution des besoins d'origine ou de l'environnement.

Ces remarques montrent qu'il est possible de distinguer trois types de maintenance :

- La maintenance de perfectionnement.
- La maintenance d'adaptation.
- La maintenance de correction.



h. Processus de management

Les processus de management assurent la cohérence du système de management de la qualité avec les orientations du contrat d'objectifs.

i. Processus de support

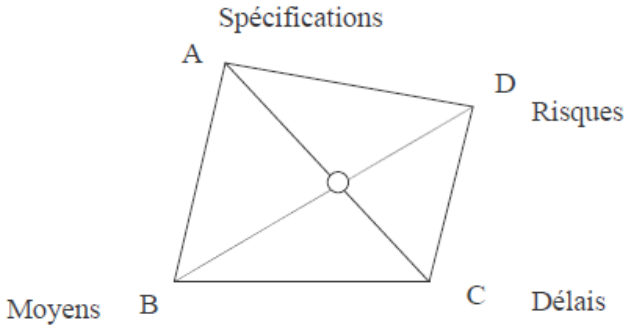
Les processus supports contribuent pour l'essentiel aux objectifs et indicateurs liés au fonctionnement et aux ressources définis dans le contrat d'objectifs.

j. management des processus

Le projet informatique

- Un projet est un ensemble de tâches dépendantes concourant à la réalisation d'un objectif unique et mesurable avec :
  - Des spécifications et des contraintes,
  - Des moyens humains, financiers et matériels,
  - Des délais,
  - Des risques.

Le challenge du chef de projet



La conduite de projet

- Ensemble de processus permettant de maîtriser la réalisation d'un projet et de le mener à terme :
  - Découpage et description du projet en processus, en activités, en lots de travaux…
  - Définition claire des entrées, des productions attendues en sortie et des conditions de passage,
  - Répartition claire du rôle et des responsabilités des acteurs.

Management de projet

- ***Finalité :*** identifier, établir, coordonner et suivre les activités, tâches et ressources nécessaires pour produire un produit satisfaisant aux exigences
- ***Pratiques de bases :***
  - Définir le champ d'application
  - Déterminer la stratégie de développement
  - Sélectionner un modèle de cycle de vie du logiciel
  - Dimensionner et estimer les tâches et les ressources
  - Développer l'organigramme des tâches
  - Identifier les exigences d'infrastructure
  - Établir le calendrier du projet
  - Allouer les responsabilités
  - Identifier les interfaces
  - Établir et mettre en œuvre des plans de projet
  - Suivre l'avancement par rapport au plan

Le plan de management

- Le plan de management permet au chef de projet d'expliciter la conduite du projet et les principes organisationnels

1- Présentation du projet
- objectifs
- client
- contrat
- garantie
- points pénalisables

2- Plan stratégique
- technique
- méthode de développement

3- Gestion des membres de l'équipe

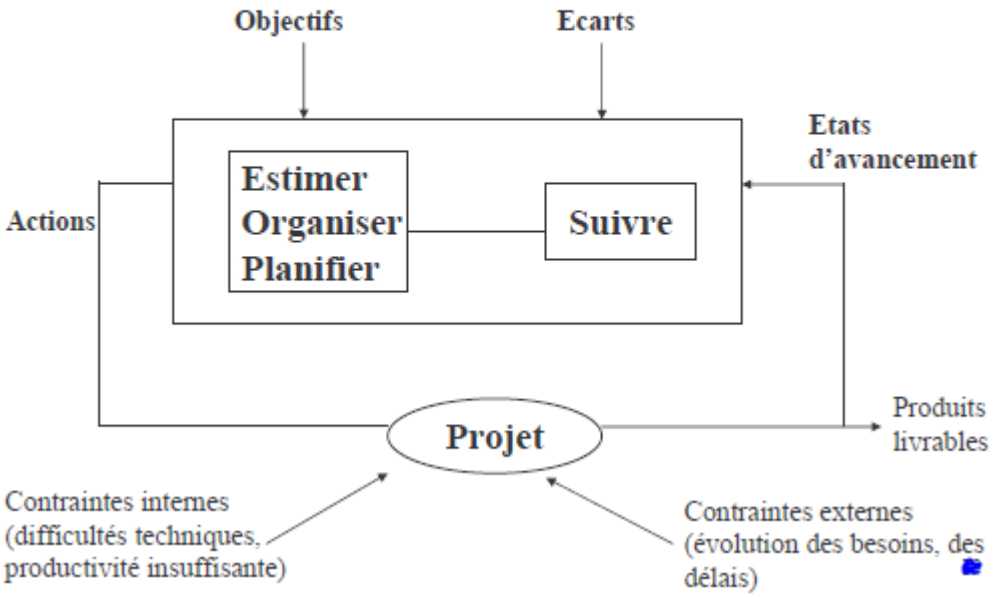
4- Plan Qualité Logiciel
- objectifs
- moyens / méthodes
- évaluation

5- Planning

6- Communication, diffusion

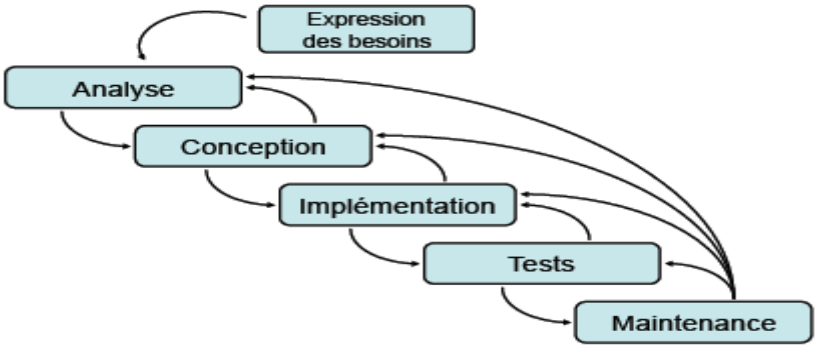
7- Pilotage
- avancement
- tableau de bords
- réunions et revues
- gestion des documents

Le déroulement du projet



IV. Types de cycle de vie

1. Cycle en cascade



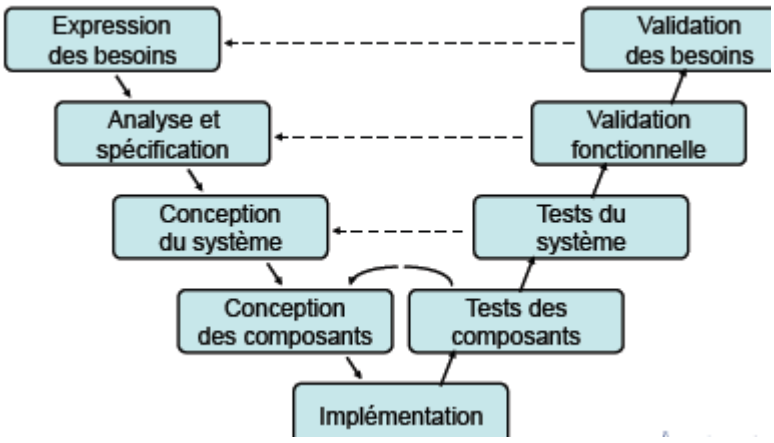
Les phases du modèle en cascade

- Expression de besoins et cahier des charges
- Spécification fonctionnelle détaillée
- Conception générale et détaillée
- Implémentation et test unitaire
- Intégration et test de conformité
- Mise en œuvre opérationnelle et maintenance

- Exemple : Merise (MCT, MCD, MOT, MLD, …)

2. Cycle en V

le cycle en V introduit la notion de décomposition et d'intégration fondamentaux dans les applications de grande taille.

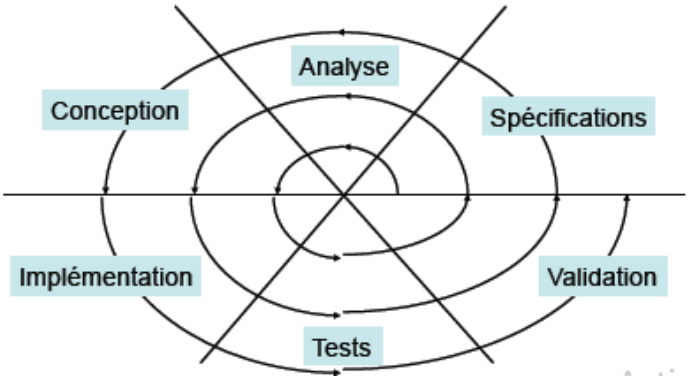


- Amélioration du modèle en cascade
- Met en évidence la symétrie et la relation qu'il y a entre les phases du début du cycle de vie et celles de fin.
- Les phases du début doivent être accompagnées d'une planification des phases de fin
- Lors de la planification, on développe et documente les plans de test.

3. Cycle en spirale

Ce type de cycle de vie s'adapte très bien aux développements par prototypes (Rapid Application Development - RAD) et en particulier aux développements dans des environnement objets (comme Smalltalk, java, Eiffel, C++).

Les risques de mauvaises analyses sont réduits par les validations fréquentes du client/utilisateur.



Mise de l'accent sur l'évaluation des risques.

A chaque étape, après avoir défini les objectifs et les alternatives, celles-ci sont évaluées par différentes techniques (prototypage, simulation, ...), l'étape est réalisée et la suite est planifiée.

Le nombre de cycles est variable selon que le développement est classique ou incrémental.

V. les différentes perceptions de la qualité.

• Validité : aptitude d'un produit logiciel à remplir exactement ses fonctions, définies par le cahier des charges et les spécifications.
  – Aptitude - exactitude - conformité réglementaire

• Fiabilité (ou robustesse) : aptitude d'un produit logiciel à fonctionner dans des conditions anormales.
  – Maturité - tolérance aux fautes - possibilité de récupération

• Intégrité : aptitude d'un logiciel à protéger son code et ses données contre des accès non autorisés.

• Réutilisabilité : aptitude d'un logiciel à être réutilisé, en tout ou en partie, dans de nouvelles applications.

• Compatibilité : facilité avec laquelle un logiciel peut être combiné avec d'autres logiciels.

• Efficacité : Utilisation optimale des ressources matérielles.
  – Comportement vis-à-vis du temps - comportement vis-à-vis des ressources

• Portabilité : facilité avec laquelle un logiciel peut être transféré sous différents environnements matériels et logiciels.

• Vérifiabilité : facilité de préparation des procédures de test.

• Extensibilité : facilité avec laquelle un logiciel se prête à une modification ou à une extension des fonctions qui lui sont demandées.
  – Facilité d'analyse - facilité de modification - stabilité

• Facilité d'emploi : facilité d'apprentissage, d'utilisation, de préparation des données, d'interprétation des erreurs et de rattrapage en cas d'erreur d'utilisation
  – Facilité de compréhension - facilité d'apprentissage - facilité d'exploitation

VI. Les 3 axes de qualité

Dans le domaine du logiciel, satisfaire les besoins de l'utilisateur suppose une démarche qualité qui prenne en compte :

- la qualité de son processus de développement (coûts, délais, méthodes, organisation, personnel, techniques, outils),
- la qualité intrinsèque du produit (modularité, simplicité, ...),
- la qualité du service fourni par le logiciel en exploitation.

La qualité du processus de développement est basée sur l'utilisation de méthodes de développement et de gestion de projet généralement définies dans le Manuel Qualité de l'entreprise rédigé au cours de la mise en place d'une politique d'assurance qualité.

L'évaluation de la qualité intrinsèque du logiciel est effectuée sur le produit en développement en fonction des facteurs de qualité attendus, définis lors de la commande (spécifications).

Celle du service porte sur le logiciel en exploitation chez l'utilisateur (ou client) et consiste notamment à vérifier son adéquation aux exigences spécifiées.

VII. Assurance Qualité

L'assurance qualité est définie comme l'ensemble des actions préétablies et systématiques nécessaires pour donner la confiance appropriée en ce qu'un produit ou service satisfera aux exigences relatives à la qualité. (NF X50-120)

En fait les moyens que l'entreprise juge nécessaire pour parvenir à la qualité souhaitée. En matière de SI, ces dispositions s'attachent à définir un cadre de production, de mise en œuvre et d'exploitation des applications.

Assurer la qualité du logiciel

- Assurer que le niveau de qualité requis est atteint
- Définir des standards de qualité et des procédures permettant d'assurer le niveau requis
- Développer une culture qualité dans les équipes de développement et de maintenance :

  "chacun est responsable"

Sept principes de la qualité

- Formalisation des procédures
  « Ecrire ce que l'on doit faire »
- Contrôle du respect des procédures
  « Vérifier que ce qui est fait est conforme à ce qui a été écrit »
- Traçabilité
  « Ecrire ce que l'on a fait »
- Mesure de la qualité
  « Apprécier la satisfaction du client »
- Calibrage par le retour d'expérience
  « Améliorer les procédures de façon continue »
- Unicité de responsabilité
  « Eviter la confusion des rôles »
- Séparation du contrôle et de la production
  « Eviter d'être juge et partie »

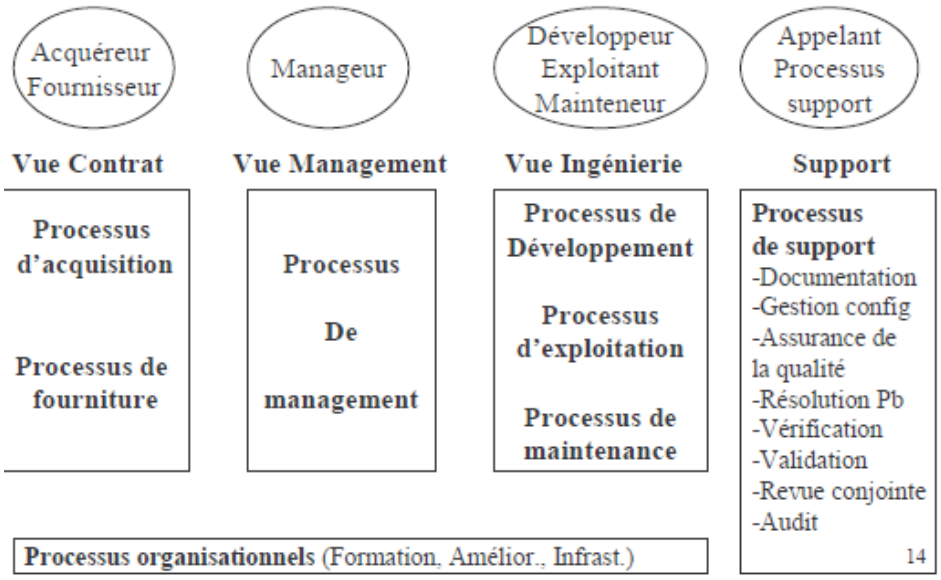
Processus d'assurance de la qualité

- Le processus d'assurance de la qualité doit fournir l'assurance que les produits du travail et les activités du projet sont conformes à leurs exigences et satisfont aux plans établis

« processus qui vise à garantir que les autres processus et les logiciels associés au cycle de vie du projet sont conformes aux exigences requises et respectent les plans pré-établis »

« il convient que ce processus soit coordonné avec les processus de vérification, de validation, de revue conjointe et d'audit »

Processus NF ISO/CEI 12.207



Manuel Qualité Logiciel

- Dispositions générales prises par une entreprise pour obtenir la qualité de ses produits et de ses services, sans tenir compte des exigences qualité d'un client ou des techniques et des outils d'un projet
  - Les règles de gestion de la qualité du logiciel,
  - Les règles et procédures en matière de conduite de projet, de production du logiciel, d'opération de tests…
  - Les plans types de documentation,
  - Ses propres règles d'évolution et l'organisation associée.
- Manuel des procédures peut être distinct

Plan d'Assurance Qualité (PAQ)

- Etabli à partir du Manuel Qualité Logiciel et des caractéristiques d'un projet déterminé doté de ses propres exigences de qualité
- Décrit les procédures, les règles et les méthodes applicables au projet
- Fixe aux différents acteurs du projet leurs droits mais aussi leurs devoirs en matière de qualité
- L'établissement et le suivi du Plan Qualité Logiciel sont du ressort du Responsable Qualité du Projet

Le Plan d'Assurance Qualité (PAQ)

- Les objectifs qualité du projet
  - Hiérarchiser les critères
- Les moyens de la qualité
  - Quelles étapes de développements (cycle de vie)
  - Choix de méthodes et techniques
  - Structuration de l'équipe
- Le suivi de la qualité
  - Quelle mesure
- Identification des risques et prévention

☞ Le document de Plan d'Assurance Qualité possède un aspect contractuel

Exemple de PAQ

1. Introduction
   - Contexte, périmètre, procédures associées au PAQ
2. Glossaire et abréviations
3. Organisation
   - Rôles des intervenants et des structures de pilotage
4. Démarche de développement
   - Activités, documents en entrée et en résultat
5. Documentation
   - Identification, contenu, validation
6. Procédures diverses
   - Gestion de configuration, gestion de projet, gestion de points en suspens, gestion des modifications, gestion des écarts du progiciel, gestion des risques, gestion des validations, gestion de la recette
7. Reproduction, Protection, Livraison
8. Suivi de l'application du plan qualité

Assurance qualité : au niveau du projet

- Spécification de la qualité du produit et du processus de développement en début de projet

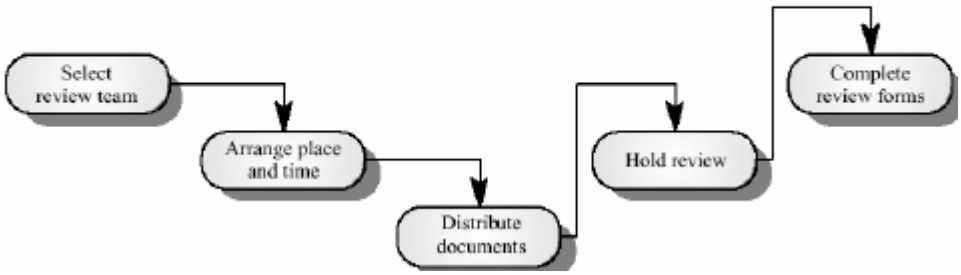
⇨ Plan d'Assurance Qualité

- Mise en œuvre des dispositions préétablies et systématiques du PAQ pour obtenir la qualité requise
- Suivi et évaluation de la qualité
  - À la fourniture des livrables, examen de la conformité,
  - Ponctuellement, conduite des revues et des audits,
  - De façon continue, appréciation de l'implication des acteurs et de l'efficacité de l'organisation
- Prévention des risques de non qualité

VIII. Contrôle de qualité

Contrôle Qualité : revues de projet

- Le groupe qualité examine avec précision les aspects méthodes et le logiciel produit ainsi que la documentation associée.
- Le code, la conception, les spécifications, les plans de test, les standards utilisés, etc. sont examinés.
- Le groupe qualité établi des recommandations qui doivent être mises en œuvre et vérifiée lors de l'audit suivant.



Revues de projet

- Equipe qualité : ingénieur qualité, chef de projet, responsable interface client
- L'objectif est de détecter, en amont, les défauts et inconsistances dans les documents et logiciels produits ainsi que dans les procédures
- Les résultats de la revue de projet :
  - Corrections à réaliser. Les concepteurs ou programmeurs doivent corriger les fautes identifiées
  - Modifications dans les méthodes de travail
  - RAS. Pas de corrections demandées

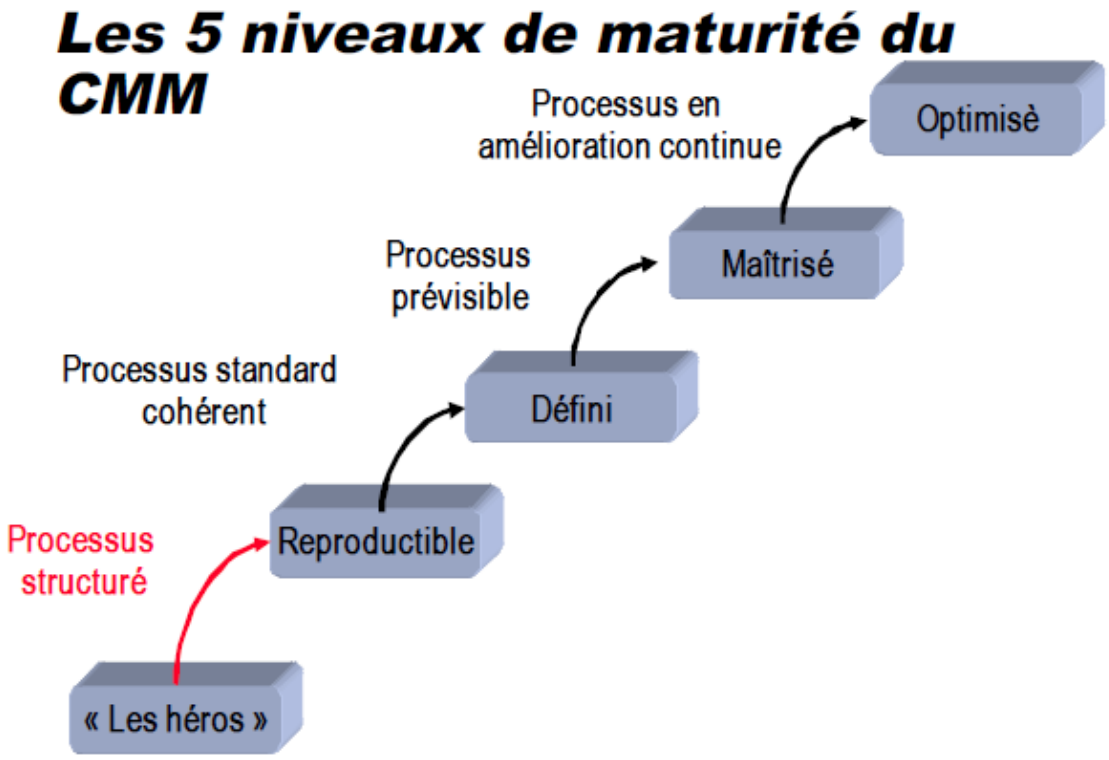
IX. Des méthodes d'évaluation etd'évolution des organisations

CMM (Capability Maturity Model)

- Mis au point par Software Engineering Institute
- Standard; version française sur http://www.CRIM.ca

SPICE

- (Software Process Improvement Capability dEtermination)
- Norme Internationale qui évolue parallèlement à la norme ISO 9000



niveau	caractéristiques	problèmes clés	résultat
5. optimisé	feedback dans le processus	automatisation	product. & qualité
4. géré	mesures	anal. et préven. des problèmes	
3. défini	mesures définies	utilisation	
2. répétable	intuition	formation, std	
1. initiation	ad hoc/ chaotique	AQL, gestion,...	risque

Niveau « 2 » reproductible :

secteurs clés

- Gestion des exigences
- Planification de projet
- Suivi et supervision de projet

- Gestion de la sous-traitance
- Assurance Qualité
- Gestion de la configuration

Maturité et normes de développement

Consensus dans l'entreprise sur la manière de faire mais pas de formalisation
Gestion rigoureuse des

Niveau « 3 » Défini : secteurs clés

- Focalisation organisationnelle
- Définition du Processus
- Programme de formation
- Coordination intergroupes
- Revue par des pairs

Processus de développement formalisé et documenté
Service de définition et de suivi des méthodes de l'entreprise

Niveau « 4 » Maîtrisé : secteurs clés

- Gestion de la qualité logicielle
- Gestion quantitative de processus
- Gestion des changements technologiques,
- Prévention des défauts
- …

Maturité et normes de développement

Niveau « 5 » Optimisé : secteurs clés

Gestion des changements technologiques,

- Prévention des défauts

Processus formel de collecte d'informations pour mesurer
le processus d'élaboration de systèmes ainsi que les produits résultants
Utilisation des résultats de la métrologie pour améliorer les méthodes

X. Types de Menaces

1. Virus

Risques

Un virus informatique est un programme conçu pour se dupliquer ; il se propage par tous les moyens d'échange de données numériques (Internet, réseau, disquette, cédérom, clé USB…) ; les effets d'un virus sont très variés, de l'affichage d'un simple message anodin à la destruction complète de toutes les données de l'ordinateur.

Protections

Les antivirus sont des logiciels conçus pour repérer les traces d'activité des virus, les bloquer et isoler ou supprimer les fichiers qui en sont responsables. Leur mode de fonctionnement est basé sur une veille permanente, à deux niveaux :

- sur tout ordinateur, un programme antivirus doit être installé et actif.
- cet antivirus doit être tenu à jour : la surveillance par l'antivirus se réfère à une base de données contenant les signes d'activité de tous les virus connus. Chaque jour, de nouveaux virus apparaissent, inventés par des experts en programmation désireux d'éprouver leurs compétences ; en permanence, d'autres experts surveillent l'apparition de ces nouveaux programmes et conçoivent des antidotes. On comprend qu'un antivirus ne sera efficace que s'il est régulièrement actualisé, pour détecter les manifestations de tous les nouveaux virus.

2. Chevaux de Troie / backdoors

Risques

Voisin des virus, un cheval de Troie (aussi appelé troyen ou trojan) est un programme qui, sous les apparences d'un logiciel utile, autorise l'exécution de commandes sur votre ordinateur, depuis un ordinateur distant, via Internet.

Certains chevaux de Troie, les backdoors, permettent de contrôler à distance votre ordinateur : après avoir infecté votre machine (lors du téléchargement d'un fichier ou l'ouverture d'une pièce jointe), le programme permet, lorsque vous êtes en connexion Internet, d'avoir un accès libre en lecture, écriture ou suppression à la totalité des fichiers présents sur votre disque dur mais également de faire exécuter à votre ordinateur des actions illégales (attaques de serveurs, intrusions dans des sites sensibles…).

Protections

Un antivirus (à jour) permet de limiter les risques d'infection.

Un firewall (matériel ou logiciel) permet, en plus, de surveiller le trafic sur votre accès Internet, pour détecter les tentatives de connexion non volontaires. En cas d'accès permanent (ADSL), il est indispensable d'utiliser un firewall qui filtre le trafic entre votre réseau local et Internet.

3. Spyware

Risques

Un spyware (ou logiciel espion) est un programme conçu pour collecter des données personnelles sur son utilisateur et les envoyer, à son insu, à un tiers via Internet.
Les spywares ne sont pas des virus parce qu'ils ne mettent pas en danger l'intégrité du

système, des applications et des données. Mais leurs actions posent des problèmes éthiques et juridiques, quant à la violation de la vie privée.

Les adwares sont des spywares qui utilisent les données récoltées (pages web visitées, essentiellement) pour afficher des publicités ou envoyer des mails ciblés ; certains sont capables de modifier la page par défaut de votre navigateur.

Les spywares sont généralement inclus dans des logiciels utilitaires : logiciels P2P (Kaaza, e-Mule…), lecteurs de médias (DivX) en sont des vecteurs connus. Mais certains fabricants de matériels et de logiciels commerciaux en incluent dans leurs produits.

Les cookies sont également des fichiers qui recueillent des informations sur la navigation des internautes mais ils ne servent qu'à faciliter la navigation dans un site donné ; ils restent, en principe, stockés sur le disque dur de l'utilisateur et ne sont pas transmis à des tiers.

Protections

La relative innocuité des spywares a conduit les fabricants d'antivirus à les négliger et des logiciels spécifiques souvent gratuits se sont développés. Les anti-spywares, comme les antivirus, utilisent des bases de données fréquemment mises à jour.

- sur tout ordinateur, un anti-spyware doit être installé et actif.
- cet anti-spyware doit être tenu à jour : la plupart des anti-spywares sont actualisables en ligne,
- sur le site de leur éditeur.

4. Spams

Risques

Le spam (ou pourriel) désigne l'envoi massif de courriers électroniques, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes. C'est un phénomène d'ampleur puisqu'on estime que 30 à 40% des mails circulant sur Internet seraient des spams.

Il existe un important trafic souterrain de listes d'adresses électroniques qui permet à des ordinateurs d'adresser un nombre énorme de mails en peu de temps.

Les produits les plus vantés sont les sites pornographiques, les médicaments, le crédit financier ou des escroqueries prétendant enrichir rapidement. Une autre forme de spam (appelée phishing) consiste à tromper le destinataire en faisant passer le message pour un message de sa banque ou d'un quelconque service protégé par mot de passe. Le but est de récupérer les données personnelles des destinataires (notamment des mots de passe) en les attirant sur un site factice enregistrant leurs actions.

Protections

Il est difficile, au niveau de l'utilisateur, de lutter contre les spams ; quelques mesures de prévention sont, toutefois, possibles :

- ne pas donner son adresse mail sur un site inconnu

- ne pas répondre aux messages de spam ni cliquer sur les liens qui prétendent vous désabonner de ces courriers.

Les serveurs de messagerie des fournisseurs d'accès Internet sont équipés de logiciels antispams qui analysent les messages et limitent l'arrivée, dans votre ordinateur, de ce type de mails.

5. Hoaxes

Risques

Il existe de faux virus, appelés hoaxes : un hoax se présente, en général, sous la forme d'un mail d'alerte contre un nouveau virus ; le message se réclame souvent d'un fabricant connu d'antivirus ou de matériel informatique, il signale un fichier dangereux et vous conseille de le détruire et demande qu'on diffuse largement l'information.

Le but des hoaxes est le simple plaisir, pour leurs concepteurs, de constater l'affolement et les encombrements provoqués par leur "plaisanterie".

Protections

Lors de la réception d'un message douteux de ce type, avant de supprimer un fichier essentiel de Windows et d'alerter tout votre carnet d'adresses, renseignez-vous… On peut trouver, sur Internet, des sites d'information sur ces fausses alertes.

6. Problèmes utilisateurs

Risques

Les utilisateurs, eux-mêmes, peuvent être à l'origine de pertes de données : par malveillance (peu fréquent, dans le cadre scolaire, beaucoup plus en entreprise) ou par maladresse. Documents non enregistrés, effacés ou perdus lors de manipulations hasardeuses sont source d'importantes pertes de temps et d'animosité à l'égard de l'outil informatique.

Protections

La protection contre ce risque passe par une connaissance de base du fonctionnement d'un ordinateur et, en particulier, du système de fichiers (notions d'arborescence, dossier, fichier…). Des habitudes efficaces et bien maîtrisées de création et d'enregistrement des documents sont indispensables : création des documents directement dans un dossier adapté, enregistrement à intervalles réguliers pendant le travail, maîtrise des opérations de copier/couper/coller limitent les risques de fausse manœuvre.

7. Mots de passe

Risques

Un certain nombre de ressources sont protégées par mots de passe pour garantir que leur utilisation reste le fait de personnes autorisées : accès à un ordinateur voire à certains dossiers et fichiers, connexion Internet, accès à une boîte de messagerie, accès à certaines pages web…

Le vol de mot de passe (par simple lecture s'il est placé à un endroit trop facilement accessible ou par "devinette" s'il est trop simple) permet à un usager non autorisé d'accéder à des outils ou à des données qui ne le concernent pas ; l'usage qu'il peut en faire serait alors imputé à l'utilisateur dont il a usurpé le mot de passe.

Protections

Le caractère relativement peu sensible des données d'une école ne nécessite pas une politique très contraignante en matière de mots de passe. Mais un minimum de sécurité et de confidentialité est recommandé :

- l'accès à l'ordinateur de gestion devra être protégé par un mot de passe puisqu'il contient des données confidentielles sur les élèves.
- ce mot de passe ne sera pas affiché sur un post-it, collé sur l'ordinateur…

Pour des raisons de sécurité mais aussi de re-paramétrage en cas de problème, il est prudent de conserver l'ensemble des mots de passe de l'école en lieu sûr (nom d'utilisateur et mot de passe, qui vont ensemble, pour la connexion Internet, les boîtes de messagerie et les accès aux ordinateurs protégés).

8. Partages

Risques

L'intérêt principal d'un réseau est le partage des ressources : dossiers et fichiers, accès Internet, imprimantes… Par défaut, lors de l'installation d'un réseau, rien n'est partagé, ce qui permet de n'ouvrir à l'accès depuis une autre machine que pour les ressources souhaitées, en les protégeant éventuellement par un mot de passe. Les risques liés aux partages sont de deux types :

- accès à des données confidentielles par des utilisateurs locaux non autorisés.
- accès à ces mêmes données et/ou prise de contrôle à distance depuis un ordinateur extérieur, via la connexion Internet.

Protections

Le partage complet des imprimantes est sans danger ; le partage de connexion Internet se met en place lors de la configuration du réseau et n'a pas à être restreint sauf si on souhaite interdire la sortie à une machine particulière ; quant au partage de dossiers, il est à définir en fonction des contenus et des utilisateurs susceptibles d'y accéder.
Il est possible d'activer le partage complet des disques des postes "élèves", ce qui facilite les transferts de fichiers ; il est cependant plus prudent de limiter ce partage à un dossier, appelé, par exemple "documents partagés", dans lequel on pourra créer autant de sous-dossiers que nécessaire, pour éviter l'accès aux dossiers système de la machine.
Pour le poste de gestion, il peut être utile de créer un dossier partagé qui permettra des échanges avec les autres postes mais il est indispensable de ne pas partager le reste du disque pour en préserver la sécurité et la confidentialité.

9. Sauvegarde

Risques

Malgré toutes les précautions prises contre les risques évoqués plus haut, il peut arriver que des données soient perdues ; le temps mis à les créer, la complexité de leur élaboration, leur caractère vital sont autant de facteurs aggravants de cette perte ; c'est pourquoi le recours à des procédures de sauvegarde est indispensable, au moins pour les données essentielles : il s'agit de conserver, en lieu sûr, une copie de ces données.

Protections

Une sauvegarde n'a de sens que si elle est :

- rigoureuse : il faut donc définir précisément les fichiers à sauvegarder ; ceci suppose une connaissance du système de fichiers de l'ordinateur et une gestion assez rigoureuse lors de l'enregistrement de vos documents. La sauvegarde de la messagerie demande de savoir localiser les fichiers qui la composent. Faute de ces connaissances, la sauvegarde sera probablement incomplète (la sauvegarde d'un disque dur entier est irréaliste).
- à jour : donc assez fréquente pour sauvegarder la dernière version de chaque document.
- récupérable : il s'agit donc d'utiliser un support et un logiciel appropriés et de les avoir testés avant d'avoir besoin d'une vraie restauration de données.

XI. Prévention du piratage informatique et moyens de protection

Document Govtech.

Le cryptage des messages (IV)

Même si en théorie il est aujourd'hui impossible pour un pirate informatique de craquer les algorithmes de dernière génération, certains systèmes de cryptage (de chiffrement) comme DES ou les signatures digitales sont vulnérables à certaines attaques. Il n'est donc pas inutile de s'attarder quelques instants sur la cryptographie.

Lorsque vous échangez des informations par Internet, en principe personne ne prend de mesure de protection particulière. Chacun présume que son correspondant est digne de confiance et que les données transmises n'ont pas été altérées.

Mais avec toutes les menaces que nous avons évoquées planant sur les communications informatiques, qui vous dit qu'en réalité la personne avec laquelle vous échangez des informations est bien la personne de confiance qu'elle prétend être ? Et qui vous garantit que le message ou le document qu'elle vous a envoyé n'a pas été modifié pendant sa

transmission ? Quelles preuves en avez-vous ? Aucune, car tout ce que vous possédez sont des données non authentiques et dont l'intégrité n'est pas garantie.

A défaut de pouvoir établir ces preuves, nous allons décrire les manières de s'assurer de l'identité des partenaires et de l'intégrité des messages. C'est le domaine du cryptage cher aux services secrets. Très complexe dans ses détails, nous nous limiterons à la description des principaux systèmes.

Le but du cryptage est de convertir un message clair en une forme codée, dite chiffrée, qui ne pourra être compréhensible sans être convertie par un processus inverse de décryptage. Cette conversion s'effectue au moyen d'algorithmes, de fonctions mathématiques et d'un mot de passe de cryptage/décryptage appelée la clé. Généralement, des lois nationales interdisent de crypter les messages, une façon pour les gouvernements de garder le contrôle et de pouvoir espionner leurs concitoyens à moindre coût.

Pourquoi utiliser les techniques de cryptage ? Le cryptage vise plusieurs buts :
- Protéger les données transitant sur des réseaux publics contre une interception ou une lecture non autorisée
- Détecter ou prévenir toute manipulation ou altération des données
- S'assurer de l'authentification de la transaction ou du document.

Parmi les limitations du système, le cryptage ne peut pas empêcher la perte ou la modification des données ni de compromettre les programmes de cryptage si la clé n'est pas suffisamment protégée. En conséquence, le cryptage consiste en une forme essentielle de contrôle d'accès mais elle est incomplète et doit de ce fait être complétée ou incoporée dans une stratégie plus globale de sécurité informatique.

Système de cryptage binaire

Entrez quelques mots dans la fenêtre du haut puis cliquez sur *Crypter* pour obtenir le résultat codé dans la fenêtre du bas. Pour décrypter le message, entrez le texte crypté dans la fenêtre du bas (ou laissez-le crypté tel quel mais effacez le contenu de la fenêtre du haut) et cliquez ensuite sur *Décrypter*.

Message décrypté: **Crypter**

Message crypté: **Décrypter**

Cet algorithme mis au point par Matthew Tong en 2002 est pratiquement impossible à craquer. La publication de cette routine sur Internet pose dès lors un problème de sécurité aux services de renseignements que nous saluons au passage. En effet, cet outil permet à chacun d'envoyer des messages

cryptés dont le double cryptage binaire empêche son déchiffrement à quiconque ne dispose pas de la clé de décryptage. Celle-ci est toutefois rendue publique en la circonstance, ce qui devrait rassurer nos gouvernements. Jusqu'à preuve du contraire, en démocratie chacun a le droit de protéger le contenu de ses communications privées s'il souhaite restreindre sa diffusion ou asurer sa confidentialité, quand bien même le message transiterait par un réseau public tel qu'Internet.

Les composantes d'un système de cryptage

Tout système de cryptage se compose de 3 éléments :

- Un algorithme de cryptage : une fonction ou un calcul mathématique permettant de crypter/décrypter les données
- Une clé de cryptage : une information utilisée par l'algorithme de cryptage rendant le processus de cryptage/décryptage unique. Similaire au mot de passe, l'utilisateur doit disposer de la bonne clé pour accéder ou déchiffrer le message. L'utilisation d'une mauvaise clé permettra de déchiffrer le message mais il sera incompréhensible.
- La longueur de la clé : définie en bits, elle détermine la difficulté avec laquelle on pourrait briser le code en essayant tous les combinaisons possibles.

L'efficacité d'un système de cryptage dépend de plusieurs critères :
- la complexité (la "force") de l'algorithme
- le secret et la difficulté de compromettre la clé
- l'absence de portes dérobées (backdoors) permettant de crypter/décrypter un fichier sans connaître la clé
- l'incapacité à déchiffrer la totalité du message si une partie de celui-ci est décryptée
- les propriétés du message connues du pirate.

Les systèmes de cryptage garantissent quatre propriétés des messages :
- La confidentialité : le secret de l'information
- L'intégrité : le fait que le message n'a pas été modifié pendant la transmission
- L'authentification : la vérification de l'identité de l'émetteur ou du destinataire
- La non-répudiation : prouver que l'émetteur ou le destinataire est bien la personne qu'il prétend être.

Ces quatre attributs sont rassemblés sous le nom d'Infrastructure à Clé Publique ou PKI en anglais.

Notre cadre étant défini, voyons à présent les deux systèmes de cryptage :
- Le cryptage symétrique (à clé privée)
- Le cryptage asymétrique (à clé publique).

Le cryptage à clé privée

Les systèmes de cryptographie à clé privée sont basés sur un algorithme de chiffrement symétrique : l'utilisateur utilise une clé secrète (privée) pour crypter le message et utilise la même clé pour le décrypter. On dit que la clé est symétrique car la clé de cryptage est la même que la clé de décryptage.

Le système de cryptage à clé privée le plus commun est le Data Encryption Standard ou DES mis au point en 1993 par le Département du Commerce américain.

DES est basé sur un algorithme public qui convertit un message en blocs (groupes ou chaînes) de 64 bits : une clé de 56 bits est utilisée pour crypter et décrypter le message

tandis que 8 bits supplémentaires sont utilisés pour vérifier la parité. Cette clé de 56 bits permet de créer 2^{56} clés différentes, soit plus de 72 millions de milliards de combinaisons.

Avec autant de possibilités, trouver la bonne combinaison semble a priori impossible mais un ordinateur suffisamment puissant peut facilement la trouver en un temps raisonnable en appliquant la force brutale, c'est-à-dire en essayant toutes les combinaisons possibles.

Ce type de clé privée pouvant être compromis à moindre frais, le système DES a été remplacé par RC2 puis RC5 et pour finir par RC6 en 1996. Il fut soumis au NIST pour devenir en 2000 le nouvel algorithme à clé privé AES (Advanced Encryption Standard) dont la clé est basée sur l'algorithme Rijndael créé par deux cryptographes belges. AES supporte des clés de 128, 192 et 256 bits.

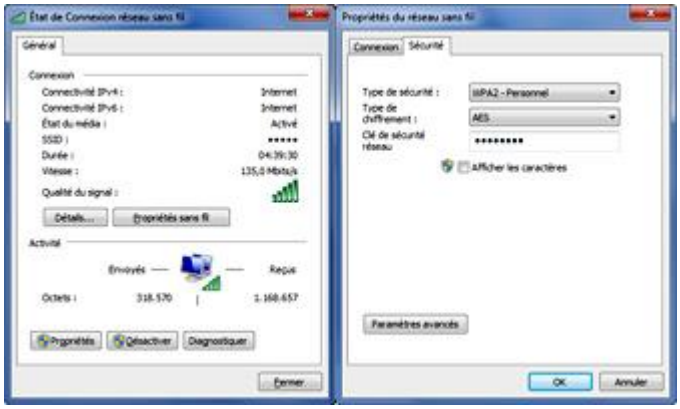
Selon une étude publiée par Microsoft en 2011, en théorie l'encryption AES sur 128 ou 256 bits pourrait être crackée. Mais rassurez-vous, comme le précisent les auteurs, "*la méthode, reste très complexe et difficilement réalisable en utilisant les technologies actuelles. Avec mille milliards de machines, chacune pouvant tester un milliard de clés par seconde, cela prendrait plus de deux milliards d'années pour récupérer une clé AES 128 bits*". Ouf, nous voilà à l'abri des pirates !

La technologie Wi-Fi cryptée

A l'ère des systèmes mobiles, il est intéressant de rappeler qu'à l'origine, vers 1999, la sécurité des télécommunications Wi-Fi sur les ordinateurs portables était assurée par le protocole WEP (Wired Equivalent Privacy) puis par WPA (Wi-Fi Protected Access). Mais l'algorithme de chiffrement RC4 n'était pas assez robuste.

En effet, la clé de 64 bits était composée d'une clé de chiffrement de 40 bits et d'un vecteur d'initialisation de 24 bits pouvant être cracké avec des programmes du commerce.

On inventa des clés de 128 et 256 bits mais elles restaient vulnérables à une attaque par la force brutale à cause des faiblesses de l'algorithme RC4. Ainsi, en 2005, le FBI a cracké la clé de 128 bits du protocole WEP en 3 minutes.



Sécurisation (authentification WPA2 et chiffrement AES) d'une connexion Wi-Fi sous Windows 7.

Conscient de cette vulnérabilité, la Wi-Fi Alliance a amélioré le protocole WPA et le remplaça à partir de 2004 par WPA2-PSK combinée au chiffrement AES sur 128, 192 et 256 bits qui fut certifiée en 2003 et standardisée dans la norme IEEE 802.11i en 2004. Grâce à cette technologie, cette fois la clé de chiffrement est pratiquement inviolable.

Point de vue pratique, la norme Wi-Fi et la technologie WPA2 AES n'ayant été normalisés que récemment, seuls les ordinateurs utilisant un système d'exploitation conçu à partir de 2005 (Windows XP, Mac OS 8.6, l'iOS 6 et les versions plus récentes, les drivers WPA2 de Linux Ubuntu et de PC-BSD ainsi que certains appareils mobiles) supportent la technologie d'authentification WPA2 et le chiffrement AES. Voir également l'article en anglais sur la configuration WPA-PSK sous Windows.

Les systèmes plus anciens présentent donc des vulnérabilités qu'un pirate équipé des bons logiciels peut rapidement exploiter.

En complément du chiffrement, sur le routeur Wi-Fi, et ce d'autant plus s'il est connecté à un serveur public sans autre sécurité (DMZ), il est important d'activer certaines options préventives comme celle cachant votre routeur (SSID=1), de désactiver les accès LAN/WAN sur le canal de la téléphonie, de désactiver les mises à jour automatiques (c'est un choix), de restreindre les connexions aux seuls périphériques que vous utilisez et dont la MAC adresse est connue et d'empêcher les accès anonymes (invité ou "guest") comme on le voit ci-dessous.

Connectez-vous à distance à votre routeur Wi-Fi : Fritz!box - Cisco/Linksys - Netgear/TP-Link
Uniquement accessible via Internet et en ayant un compte sur un serveur NAS

Trois parmi les nombreux écrans de configuration d'un routeur Wi-Fi Fritz!Box 7390 dont voici le manuel en français. Ces paramètres (remplacés par des valeurs fictives pour l'exemple) permettent d'augmenter la sécurité de l'authentification et des accès Wi-Fi. A gauche, la configuration du cryptage WPA2, au centre la suppression (non activation) du nom du routeur (SSID) et la restriction des périphériques Wi-Fi aux seuls connus, et à droite l'inactivation de la possibilité d'avoir des utilisateurs invités (guest).

De nos jours, la technologie WPA2 AES est en principe activée sur tous les ordinateurs et smartphones connectés par Wi-Fi et vous met à l'abri de tout piratage sur la ligne reliant votre système au routeur Wi-Fi ou au hot spot, mais pas entre le routeur et votre opérateur ni vers Internet où le trafic passe par l'infrastructure publique, non sécurisée.

Pour protéger ce segment de toute intrusion venant d'Internet ou de la ligne vous reliant à votre fournisseur d'accès, il est prudent d'installer en complément un firewall (pare-feu) software, souvent inclus dans votre OS, ainsi qu'un logiciel anti-virus et anti-phishing sur votre système.

A l'avenir, toutes les applications et les protocoles devraient supporter l'encryption AES pour l'échange sécurisé d'information. L'utilitaire BitZipper par exemple supporte l'encryption AES.

L'avantage du cryptage à clé privée est que l'utilisateur ne doit disposer que d'une seule clé pour le cryptage et le décryptage. Le système à clé privée est également moins compliqué et requiert donc moins de traitements, moins de ressources CPU qu'un système asymétrique. Il est donc adapté au cryptage de quantités importantes de données.

Désavantages, il est difficile d'échanger des clés privées par Internet et plus encore avec toute une communauté, notamment dans le e-commerce où les clients sont inconnus ou dont vous ignorez le degré de confiance. Pire, la clé symétrique ne peut pas être utilisée pour signer électroniquement un document ou un message car ce mécanisme est basé sur le partage d'un secret. On y reviendra.

Le cryptage à clé publique

Pour résoudre ces deux problèmes, les mathématiciens ont inventé des systèmes de cryptographie à clé publique basés sur un algorithme de cryptage asymétrique. Cette solution permet au propriétaire (par exemple à l'entreprise) de disposer d'une clé privée et de distribuer autant de clés publiques qu'il y a de clients tout en échangeant des informations de manière sécurisée. Arrêtons-nous un instant sur ce système car il a le mérite d'être pratiquement inviolable.

Les deux clés fonctionnent ensemble comme une paire. Une clé est utilisée pour crypter les données, l'autre clé est utilisée pour les décrypter. L'une ou l'autre clé peut servir à crypter ou décrypter les données, mais une fois que la première clé est choisie pour crypter les données, seule la seconde clé peut être utilisée pour les décrypter.

Le cryptage asymétrique offre un grand confort aux personnes achetant sur Internet. En effet, la clé privée appartenant au web marchand et la clé publique étant distribuée aux clients, ces derniers peuvent en toute confiance s'assurer de l'identité (l'authentification) du web marchand et ce manière pratiquement transparente (il faut parfois valider un certificat, voir plus bas).

Concrètement, le web marchand dispose de la clé privée avec laquelle il va crypter son message. Le client va le décrypter en utilisant la clé publique. Inversement, le client lui répondra en cryptant son message avec la clé publique et le web marchand va le décrypter avec la clé privée.

Les clés sont asymétriques car elles sont en relation inverse l'une par rapport à l'autre. L'algorithme de cryptage est basé sur la factorisation d'un nombre entier, l'idée étant de générer un produit à partir de deux nombres premiers, sachant qu'il est pratiquement impossible de factoriser le nombre résultant pour retrouver les deux facteurs.

On en conclut que s'il est relativement aisé d'effectuer le calcul dans une direction, il devient très difficile voire pratiquement impossible de le réaliser dans l'autre direction. Ce genre de cryptage est donc très fiable et sa simplicité n'est qu'apparente. Car les calculs prennent en considération l'arithmétique modulaire, les exposants et des nombre premiers de milliers de bits de longueurs !

A choisir entre un système à clé symétrique ou asymétrique, il faut savoir que le temps de cryptage augmente de façon disproportionnée en fonction de la complexité de la clé. Ainsi, en passant d'une clé de cryptage asymétrique de 512 bits à 1024 bits, le temps de décryptage devient 6 fois plus long.

De part la lenteur du traitement, les clés asymétriques sont généralement utilisées pour crypter des messages courts comme le cryptage des clés symétriques DES ou pour créer des signatures digitales. C'est pourquoi elles sont souvent utilisées pour crypter les résumés ou "digest" des messages ou les signatures (voir plus bas).

La forme la plus connue de cryptage asymétrique est RSA, un système de cryptage à clé publique inventé en 1977 par Rivest, Shamir et Adleman. En pratique, à partir de la clé publique il est extrêmement improbable de retrouver la clé privée en raison du problème posé par la factorisation.

Toutefois, parmi les nombreux algorithmes de factorisation existants, l'algorithme NFS (Number Field Sieve) permet de factoriser des grands nombres à l'instar du fameux "Crible d'Ératosthène". Les pirates s'en servent donc également pour attaquer les systèmes de cryptage RSA. Il y a même des compétitions de factorisation de nombres RSA.

Parmi les autres systèmes de cryptage asymétriques, citons le cryptage par courbe elliptique (ECC) développé à partir de 1985 par Neal Koblitz et Victor Miller. De quoi s'agit-il ?

Les courbes elliptiques sont des objets mathématiques utilisés pour effectuer des opérations asymétriques comme des échanges de clés sur un canal non sécurisé ou le cryptage asymétrique. Une courbe elliptique peut être définie suivant l'équation suivante : $y^2 = x^3 + ax + b$.

Les algorithmes ECC sont basés sur la difficulté de trouver un logarithme discret dans un champ fini; il est en effet plus difficile de calculer un logarithme discret sur une courbe elliptique que de factoriser le produit de grands nombres.

ECC est adapté aux environnements mobiles et Wi-Fi. Si les anciennes versions étaient limitées par la bande passante et la puissance du processeur (surtout sur les terminaux mobiles), aujourd'hui ce système est plus performant et offre plus de sécurité par bit. Ainsi, un système ECC disposant d'une petite clé de 160 bits offre la même sécurité qu'un système basé sur la factorisation comme RSA et exploitant une clé de 1024 bits.

Pour mémoire, citons le système cryptographique PGP (Pretty Good Privacy) inventé en 1991 par Philip Zimmermann. PGP est une solution hybride exploitant un cryptage symétrique (donc très rapide) et un système asymétrique (beaucoup plus lent) ainsi qu'une clé privée temporaire à usage unique. Inconvénient, ce système génère un message codé au moins deux fois plus volumineux que le message en clair.

Enfin, le cryptage quantique tente de résoudre les problèmes des systèmes de cryptage actuels. Toujours à l'état de prototype chez British Telecom et IBM notamment, nous y reviendrons dans l'article consacré à l'ordinateur quantique à propos de la communication quantique.

Disons seulement que l'information peut être encodée dans l'état de polarisation des photons, rendant son piratage illusoire. Le jour où ce système sera commercialisé, les pirates devront trouver d'autres manières de passer le temps !

La signature digitale

La signature digitale est un identification électronique d'une personne ou d'une entité créée au moyen d'un algorithme à clé publique qui permet au destinataire de s'assurer de l'intégrité des données et de l'identité de l'expéditeur.

Sans entrer dans les détails, pour garantir l'intégrité des données, le système va procéder en trois étapes.

1ere étape

D'abord un algorithme de hachage (dit fonction de hachage ou "hashing" telle que SHA-1, MD5, etc) calculé pour l'ensemble du message ou des données va générer une petite chaîne de caractères d'une taille fixe, généralement égale à 128 bits.

Ce processus qui représente la signature digitale va générer un résumé du message ou "digest". Similaire à un "checksum", il représente en quelque sorte "l'empreinte digitale" du message et est utilisé pour détecter toute altération du message.

Ces algorithmes de hachage sont à sens unique, c'est-à-dire qu'à l'inverse des algorithmes de cryptage à clé privée ou publique, à partir du résumé, on ne peut pas reconstruire le message.

Cette technique est utilisée lorsqu'on doit traiter de gros documents électroniques comme des fichiers de traitement de texte, des tableurs, des enregistrements de bases de

données, le contenu d'un disque dur ou une image et qu'ils doivent être compressés de manière sécurisée avant d'être signés avec la clé privée.

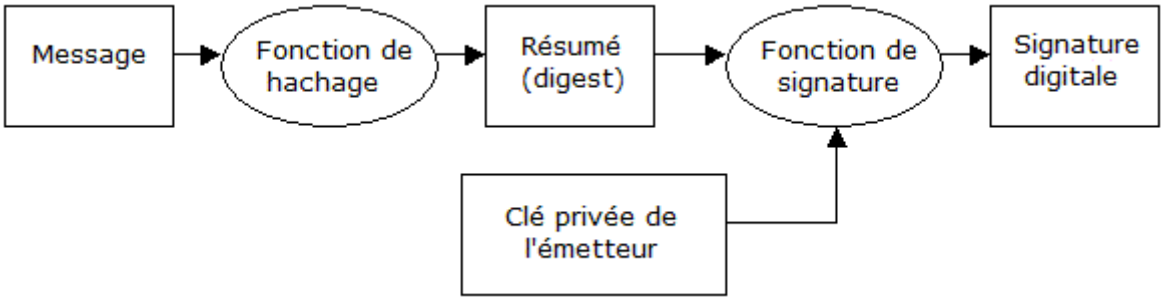
Notons que les systèmes MD4 et MD5 ont été optimisés pour les processeurs 32 bits.

2e étape

La deuxième étape consiste à vérifier l'identité de l'expéditeur. Celui-ci va crypter le résumé (digest) de son message au moyen de sa clé privée, laquelle "signe" le document avec la signature digitale prouvant l'authentification de l'expéditeur.

Le système va ensuite transmettre ensemble le message en clair et sa signature au destinataire

Schéma du processus de création d'une signature digitale par l'émetteur d'un message :



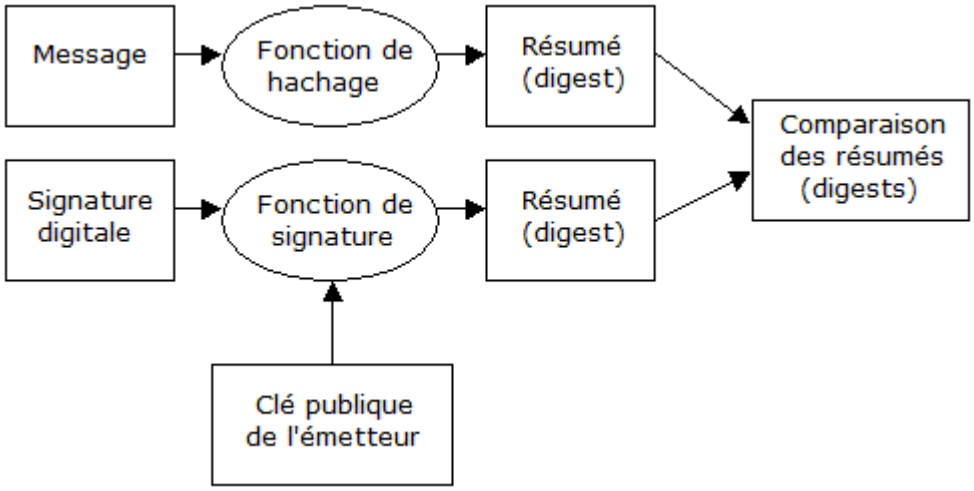
3e étape

A la réception, le destinataire va ouvrir le message. Le système va tout d'abord utiliser la clé publique de l'expéditeur pour déchiffrer sa signature digitale. S'il réussit, cela prouve que le message a bien été émis par l'expéditeur concerné. Ce processus qui authentifie l'expéditeur s'appelle la non-répudiation car l'expéditeur ne peut pas prétendre par la suite ne pas avoir généré le message.

Enfin, le destinataire va recalculer le "hash" sur l'entièreté du message en utilisant le même algorithme que l'expéditeur (la fonction de hachage) et comparer les deux résumés. Si le "hash" calculé est identique à celui déchiffré à partir de la signature digitale, l'intégrité du message est assurée; celui-ci n'a pas été altéré ou modifié au cours de la transmission. Si le message a été modifié au cours de la transmission, la signature digitale ne pourra pas être vérifiée avec succès, le résumé sera altéré et le message considéré comme corrompu et dans certains cas, il sera même illisible.

Si une fonction de hachage sécurisée est utilisée, un pirate ne pourra pas récupérer la signature du document pour la joindre à un autre document ou altérer le message signé. En effet, la moindre modification apportée à ce document signé électroniquement entraînera l'échec du processus de vérification de la signature digitale.

Schéma du processus de vérification de la signature digitale par le destinataire du message :



Documents inspirés de Youdzone.

En résumé, la signature électronique est une méthode de cryptage qui assure trois fonctions :

- L'authentification
- L'intégrité des données
- La non-répudiation.

Les signatures digitales comme les clés publiques de cryptage sont vulnérables aux attaques dites "man-in-the-middle" qui visent à intercepter les communications entre deux systèmes du fait qu'il est possible de simuler la clé privée et publique d'une signature digitale et ainsi tromper l'expéditeur et le destinataire. Pour se protéger contre de telles attaques, il faut désigner une autorité d'authentification. Cette fonction indépendante est assurée par le PKI en ce sens qu'il valide les signatures digitales de l'émetteur et les clés publiques (voir plus bas).

L'Infrastructure à Clé Publique ou PKI

Etant donné que la transmission électronique de documents cryptés fait l'objet de tentatives de piratage, pour assurer la confidentialité, l'authentification, l'intégrité et la non-répudiation des messages, un cadre de travail et une instance de contrôle ont dut être définis afin d'éviter les problèmes d'interception et de modification des clés publiques. Il s'agit de l'Infrastructure à Clé Publique ou PKI, alias Public Key Infrastructure.

Le PKI est un partenaire de confiance dont le rôle est d'émettre, de maintenir et de supprimer (révoquer) les certificats des clés publiques. Le PKI permet aux utilisateurs d'interagir entre eux et avec des applications, d'obtenir et de vérifier les identités et les clés de sources de confiance. L'installation d'un PKI varie en fonction des besoins mais comprend au minimum :

- Des certificats digitaux
- Une autorité de certification (CA)
- Une autorité d'enregistrement (RA).

Les certificats digitaux

Il s'agit d'une pièce justificatrice digitale constituée d'une clé publique et une donnée identifiant son propriétaire. Le but du certificat digital est d'associer la clé publique à l'identité d'un individu ou d'une société. Fourni sous forme électronique (de fichier à extension .cer), ils sont signés digitalement par une société de confiance avec leur clé privée (voir plus bas).

Le certificat digital s'utilise pour prouver l'authentification de l'expéditeur. Lorsqu'une personne veut signer un document pour l'authentifier ou que le système l'exigence de manière transparente, celui-ci attache un certificat digital émis par la société de confiance. Le destinataire du message (ou le système gérant la base de données) et le certificat digital attachés vont se baser sur la clé publique (qui est soit comprise dans le certificat digital soit obtenue séparément) de l'autorité de confiance du certificat pour authentifier le message.

Le certificat digital d'un utilisateur devrait toujours inclure le nom de la personne, une clé publique valide, l'algorithme utilisé pour calculer la signature électronique du certificat et la période de validité du certificat.

L'autorité de certification (CA)

Il s'agit d'une autorité qui émet et gère les pièces justificatrices de sécurité et les paires de clés publiques/privées afin que les utiliseurs puissent s'assurer de l'authenfication de la signature des messages et du cryptage.

L'autorité de certification, dans ce cas ci la société Verisign, demande à l'utilisateur s'il veut bien faire confiance (to trust) en l'authentification du certificat associé à un applet Java développé par la société Documentum qui permet de gérer des documents électroniques (fax).

Le CA atteste l'authentification du propriétaire, utilisateur ou entité, d'une paire de clé publique/privée. Il va émettre ou non un certificat digital sur base de preuves ou de connaissance obtenues après avoir vérifié l'identité du demandeur.

En collaboration avec l'autorité d'enregistrement (RA), le CA va vérifier les informations fournies par le demandeur du certificat digital. Si le RA a vérifié et validé les informations du demandeur alors seulement le CA pourra émettre un certificat. Le CA signe le certificat avec sa clé privée et la distribue à l'utilisateur. A la réception, celui-ci vérifiera la signature du certificat au moyen de la clé publique émise par le CA.

Généralement le CA est une société commerciale de confiance telle que Verisign, Certco, Cybertrust, etc. Elle émet les certificats destinés aux browser web (Internet Explorer, etc) , aux applications client-serveur, aux messageries électroniques, etc.

En plus de son activité de certification, le CA est également responsable de la gestion du cycle de vie du certificat digital. Il tient à jour la liste des certificats révoqués (CRL) et émet la déclaration de pratique de certification (CPS). Le CPS décrit les règles gouvernant les opérations de l'autorité de certification en termes de contrôles et de méthodes qu'elle utilise pour valider l'authenticité des demandeurs de certificats ainsi que la manière dont ses certificats devrait être utilisés.

L'autorité d'enregistrement (RA)

Dans une petite entreprise ou à titre privé, le CA vérifie et enregistre les demandes de certificats digitaux des utilisateurs. Mais au sein d'une grande entreprise travaillant en réseau et employant des milliers de salariés, le CA peut déléguer cette fonction administrative à l'autorité d'enregistrement ou RA.

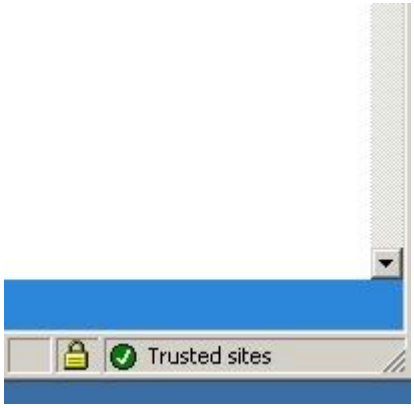
Le RA assure la fonction d'établir le lien entre l'individu ou l'entité et la clé publique. Il vérifie les informations fournies par le demandeur, son droit à demander les attributs du

certificat et le fait qu'il possède une clé privée enregistrée et qu'elle correspond à la clé publique demandée avec le certificat, ce qu'on appelle la preuve de possession (POP).

En complément, le RA tient la liste à jour des clés compromises ou révoquées, il assigne les noms, génère les codes secrets paratgés nécessaires durant la phase initiale d'enregistrement, il initialise avec le CA le processus d'enregistrement au nom du demandeur, il assure également la restauration des clés et distribue les cartes physiques (smart cards) contenant les clés privées.

Application des systèmes de cryptage

La plupart des systèmes cryptés transitant sur Internet ou sur un réseau d'entreprise utilisent une combinaison de paires de clés privées/publiques, de clés secrètes, de fonctions de hachage et de certificats digitaux.



Les paiments par Internet passent généralement par le protocole SSL sécurisé (clé de 128 bits), parfois symbolisé dans le browser Internet par le cadenas. Le certificat confirme que le site est de confiance.

Ainsi que nous l'avons expliqué, le but des systèmes de cryptage est de garantir la confidentialité, l'intégrité du message et la non-répudiation soit de l'émetteur soit du destinataire.

A titre privé par exemple, la meilleure façon d'éviter que l'on accède à des données confidentielles qui seraient sauvegardées sur votre ordinateur est de crypter votre disque dur avec votre propre clé publique. Ainsi on ne pourra accéder à l'information qu'en utilisant votre clé privée qui ne doit jamais être partagée.

La cryptographie s'applique également au cryptage des protocoles, c'est-à-dire aux règles par lesquelle un réseau opère et contrôle le flux ainsi que les priorités des transmissions. Les principaux protocoles sécurisés sont les suivants :

Ainsi, sans vous en rendre compte, si vous effectuez des paiments ou transmettez des données confidentielles par Internet, il y a de fortes chances que votre application utilise un protocole sécurisé, symbolisé par le petit cadenas qui figure en bas à droite de votre browser Internet, notamment lors des opérations de e-banking et e-commerce. Dans ce cadre, SSL est certainement l'un des protocoles sécurisés les plus utilisés.

- SSL et TLS : le "Secure Socket Layer" (SSL) et le "Transport Layer Security" (TLS) sont des protocoles qui sécurisent les communications par Internet entre browser et server web. S'ajoute à ceux-ci le "Wireless Transport Layer Security" (WTLS) dédié aux applications WAP (Wireless Application Protocol) supportées par les appareils mobiles. Bien qu'il y ait peu de différence entre SSL et TLS/WTLS, ils ne sont pas interchangeables.

  SSL et TLS/WTLS opèrent au niveau de la couche de connexion ou session de l'utilisateur. Cette technique utilise une clé publique, un échange crypté de clé et un certificat digital.

  SSL offre une protection contre les tentatives de lecture et notamment contre les sniffers, des appareils portables capables d'analyser en détail les paquets transitant sur un réseau, y compris sur Internet. SSL est utilisé dans des fonctions garantissant la confidentialité des informations telles que :

  - Le cryptage à clé privée : RC2, RC5, IDEA, DES, Triple DES, AES
  - Le cryptage à clé publique : RSA, Fortezza, etc

- La fonction de hachage (hashing) à sens unique : MD5, SHA-1, SHA-256.

Dans le modèle OSI, SSL tourne entre la couche de transport TCP qui fait partie de l'ensemble TCP/IP, et les protocoles applicatifs tels que HTTP (Internet), SMTP (e-mail) et NNTP (transfert réseau). SSL offre donc une protection à tous les protocoles utilisant TCP et en particulier pour le protocole bien connu S/HTTP utilisé pour toutes les transactions de paiment effectuées par Internet (e-banking, e-commerce, etc).

Concernant les applications WAP, ce protocole pour terminaux mobiles requiert un gateway WAP afin de permettre l'échange de messages entre topologies différentes. Seul inconvénient, les messages éventuellement cryptés envoyés par les utilisateurs doivent être décryptés pour être transmis sur Internet et vice versa. Pour éviter tout risque de piratage, ce gateway WAP doit utiliser les technologies WTLS et SSL, WTLS garantissant l'authentification, la confidentialité, l'intégrité et empêchant toute écoute indiscrète des transmissions.

Il demeure toutefois que le protocole SSL est vulnérable aux attaques "Man in the middle". En effet, un pirate peut utiliser un serveur SSL factice afin qu'il accepte les messages sous protocole SSL et ensuite dérouter le véritable serveur SSL pour intercepter les informations sensibles.

- S/HTTP : le "Secure Hypertext Transfer Protocol" opère au niveau applicatif et permet d'échanger des messages, des documents ou des pages web de manière sécurisée entre un utilisateur relié à Internet et un serveur web connecté sous le protocole SSL. HTTPS utilise des certificats à clé publique pour vérifier l'identité des émetteurs et des destinataires. Ce processus est transparent pour l'utilisateur.

  Son activation se matéralise dans le browser web par le remplaçant de l'adresse Internet (URL) traditionnelle commençant par "http://" par sa version sécurisée "https://" qui redirige le message vers un port sécurisé plutôt que vers l'adresse du port web 80: définie par défaut.

- S/MIME : le "Secure Multipurpose Internet Mail Extensions" est le protocole sécurisé standard du courrier électronique (e-mail). Il authentifie l'identité de l'expéditeur et du destinataire, vérifie l'intégrité du message et garantit le secret (privacité) du contenu du message, y compris des pièces jointes (attachments).

- SSH : le "Secure Shell" assure la sécurité des services client-server, Telnet et FTP. Ainsi, dans un contexte client-server où l'utilisateur se connecte à distance à l'application de son entreprise, SSH ouvre une session shell (en ligne de commande) sécurisée et cryptée.

  Semblable à un réseau virtuel privé (VPN), SSH encrypte les données y compris les mots de passes, les fichiers binaires et les commandes d'administration transmises entre les systèmes sur le réseau ou par Internet. A l'inverse d'IPsec qui opère au niveau de la couche réseau, SSH est implémenté dans les couches supérieures, au niveau de la couche application.

- IPSec : ce protocole est utilisé pour les communications entre deux ou plusieurs systèmes qu'il s'agisse d'ordinateurs ou de segments de réseaux (subnets). Cette couche réseau sécurisée opère au niveau IP établissant des VPN et transmettant les paquets de données dans une charge encapsulée (EPS) cryptée ou, comme dans le mode tunnel, cryptant la charge ainsi que son entête, afin d'assurer la confidentalité.

  On peut encore renforcer la sécurité d'IPSec en utilisant un cryptage asymétrique au travers du protocole ISAKMP/Oakley.

- SET : le "Secure Electronic Transactions" est un protocole développé conjointement par VISA et Master Card pour sécuriser les transactions de paiment entre parties exploitant les cartes de crédits au nom des propriétaires et des web marchands. Comme toute technologie dont les spécifications sont ouvertes, publiques, SET est un protocole orienté application qui utilise des processus de cryptage et de signatures digitales de tiers de confiance dans le cadre du PKI.

Risques associés au cryptage

Les systèmes de cryptographie restent vulnérables dès le moment où les méthodes de cryptage sont principalement fondées sur le secret. En général, plus une clé est utilisée, plus elle devient vulnérable et risque d'être compromise. Ainsi, aujourd'hui en utilisant la force brutale, un mot de passe constitué d'une clé de 40 bits (comparable à une chaîne de 10 caractères) peut-être craqué en quelques heures. Il faut donc installer une protection beaucoup plus efficace pour dissuader les pirates.

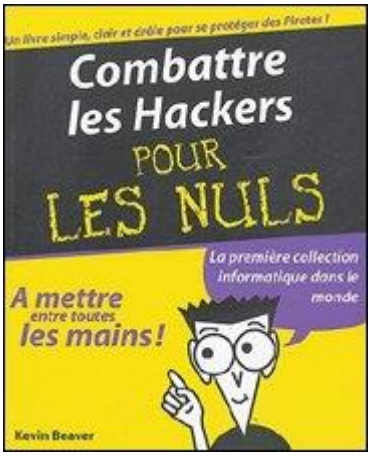
Clé signifie mot de passe. Le fait de se fier à des fonctions aléatoires ne garantit pas de créer un mot de passe fort car le système peut très bien par hasard générer une suite continue de chiffres ou des mots communs, surtout quand la longueur du mot de passe ne dépasse pas 10 caractères.

Dès lors, même un algorithme de cryptage de 128 bits peut offrir une bien maigre protection lorsque les clés de cryptage sont basées sur des mots de passes et que ces derniers manquent de robustesse (trop simples). C'est pourquoi il est important que la syntaxe des mots de passes respecte des règles strictes et que les codes faciles à retenir soient interdits.

Ainsi qu'on le constate, sans la participation et la bonne volonté des utilisateurs, la meilleure protection informatique ne sert à rien. Ayez-en conscience et rappelez-vous des bonnes pratiques lorsqu'en votre absence vous laisserez votre ordinateur entre les mains d'un inconnu ou d'une personne qui n'a pas toute votre confiance.

En guise de conclusion

Comme tout programmeur, un pirate est paresseux. Il serait idiot de réinventer la roue en cherchant des failles dans la sécurité du système ciblé, qui n'existent peut-être pas. Le pirate a intérêt à profiter des vulnérabilités existantes sur le site convoité, comme par exemple dans les systèmes CGI, HTTP et autre RSA.



Ces failles sont connues de tout bon programmeur pirate, documentées sur les forums, et parfois même signalées par les médias, comme ce fut récemment le cas avec les vulnérabilités découvertes dans l'iPhone d'Apple. Certaines vulnérabilités sont résolues (HTTPS, IPSec, WPA2 AES, signature digitale, etc) mais tout le monde ne les applique pas, souvent par méconnaissance.

Bref, un bon pirate connaît les failles du système qu'il convoite, il a parfois même ses entrées dans cette société ou profite de la naïveté d'un contact. Malin et compétent, il aura toujours une longueur d'avance sur les responsables de la sécurité informatique.

Quant au lecteur non initié, renseignez-vous sur les protections installées sur votre ordinateur, votre tablette ou votre smartphone (avez-vous déjà installé un anti-virus par exemple ?) ou consultez un expert technique auprès de votre fournisseur d'accès à Internet et protégez vos biens contre tout risque d'intrusion. Sans vous

alarmer, rappellons que les risques ne sont pas nuls et tous les jours dans chaque pays des dizaines de sociétés et des amateurs se font pirater.

Un homme averti en vaut deux.