UNIVERSITÉ PARIS 1

PANTHÉON SORBONNE

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

4.1 Sécuriser l’environnement numérique

Sommaire

- Les réseaux
- Les attaques
- Les mouchards (Spywares)
- La protection de la machine
- Les précautions à prendre

Sommaire

- Les réseaux
- Les attaques
- Les mouchards (Spywares)
- La protection de la machine
- Les précautions à prendre

Les réseaux : internet

- L'accès à internet nécessite :
  - une adresse IP : numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol.
  - un Fournisseur d'Accès à Internet (FAI) : prestataire de services offrant une connexion à internet :
    - ADSL (Asymetric Digital Subscriber Line) : permet d'utiliser une ligne téléphonique, pour transmettre et recevoir des données numériques de manière indépendante du service téléphonique conventionnel via un filtre ADSL branché à la prise ;
    - la fibre optique : fil en verre ou en plastique très fin servant dans la transmission de données et de lumière. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et peuvent servir de support à un réseau « large bande » par lequel transitent aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques ;
    - le satellite : pour les régions difficiles d'accès.

Les réseaux : modèles

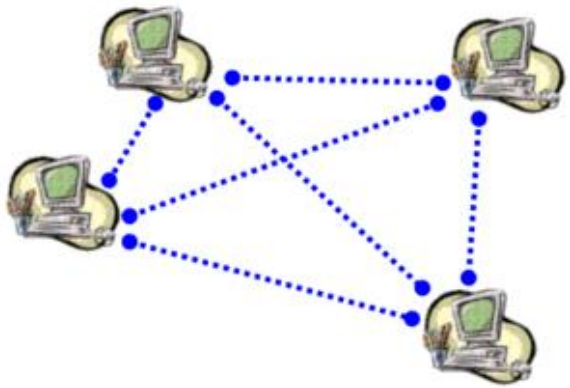
- Modèle client-serveur :
  - le serveur est un ordinateur dont le rôle est de traiter et de répondre aux requêtes envoyées par des ordinateurs clients.

- Exemples de serveurs :
  - serveur web : met à disposition des pages web ;
  - serveur FTP (File Transfer Protocol) : permet le téléchargement ou le dépôt de fichiers ;
  - serveur de messagerie : transfère le courrier électronique.

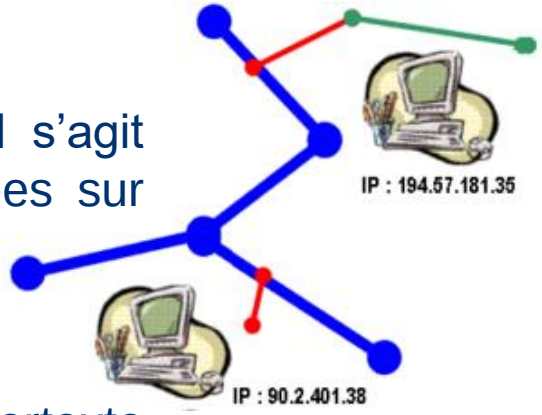
Les réseaux : modèles

Le modèle Pair-à-Pair (P2P, Poste-à-Poste, Peer-to-Peer) :

- il peut être utilisé pour des applications légales ;
- tous les ordinateurs ont le même rôle ;
- les machines échangent deux à deux des données et des services, en jouant tour à tour le rôle de client et de serveur ;
- les applications de partage de fichiers (P2P) reposent sur ce modèle.



Les réseaux : protocoles



- Le Protocole TCP/IP :
  - Transmission Control Protocol/Internet Protocol, il s'agit d'un protocole utilisé pour le transfert des données sur Internet.

- Les protocoles d'applications :
  - HTTP (HyperText Transfer Protocol) : transfert hypertexte pour naviguer sur le web ;
  - HTTPS : version sécurisée de HTTP (combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS) permet de transmettre les données de manière cryptée :
    - Exemple: messagerie de l'Université, achats en ligne ;
  - FTP (File Transfer Protocol): échange informatique de fichiers ;
  - SMTP (simple mail transfert Protocol), POP3 (Post Office Protocol), IMAP (Internet Message Access Protocol) : protocoles utilisés pour la messagerie électronique (cf D5).

Les réseaux : chiffrement

Le chiffrement

Le chiffrement d'un message permet de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. Une fois chiffré et grâce à un système de verrou, faute d'avoir la clé spécifique, le message est inaccessible et illisible, que ce soit par les humains ou les machines.

Ce procédé de cryptographie automatique :

- Assure la confidentialité des données ;
- Certifie des échanges numériques ;
- Apporte une preuve numérique qu'un document n'a pas été modifié.

Certaines messageries (Whatsapp, Télégram, Signal) utilisent le chiffrement « de bout en bout ». Ce procédé est également utilisé dans le cadre de la protection des transactions bancaires, la signature électronique de contrats, ou encore pour limiter l'accès à des contenus payants.

Sommaire

- Les réseaux
- Les attaques
- Les mouchards (Spywares)
- La protection de la machine
- Les précautions à prendre

Les attaques : définitions

- Pirate informatique (ou hacker) :
  - un hacker est un spécialiste de la sécurité informatique qui maitrise donc les moyens de déjouer cette sécurité. Certains utilisent leurs compétences pour enfreindre la loi. Dans ce cas, on parle de pirates informatiques.

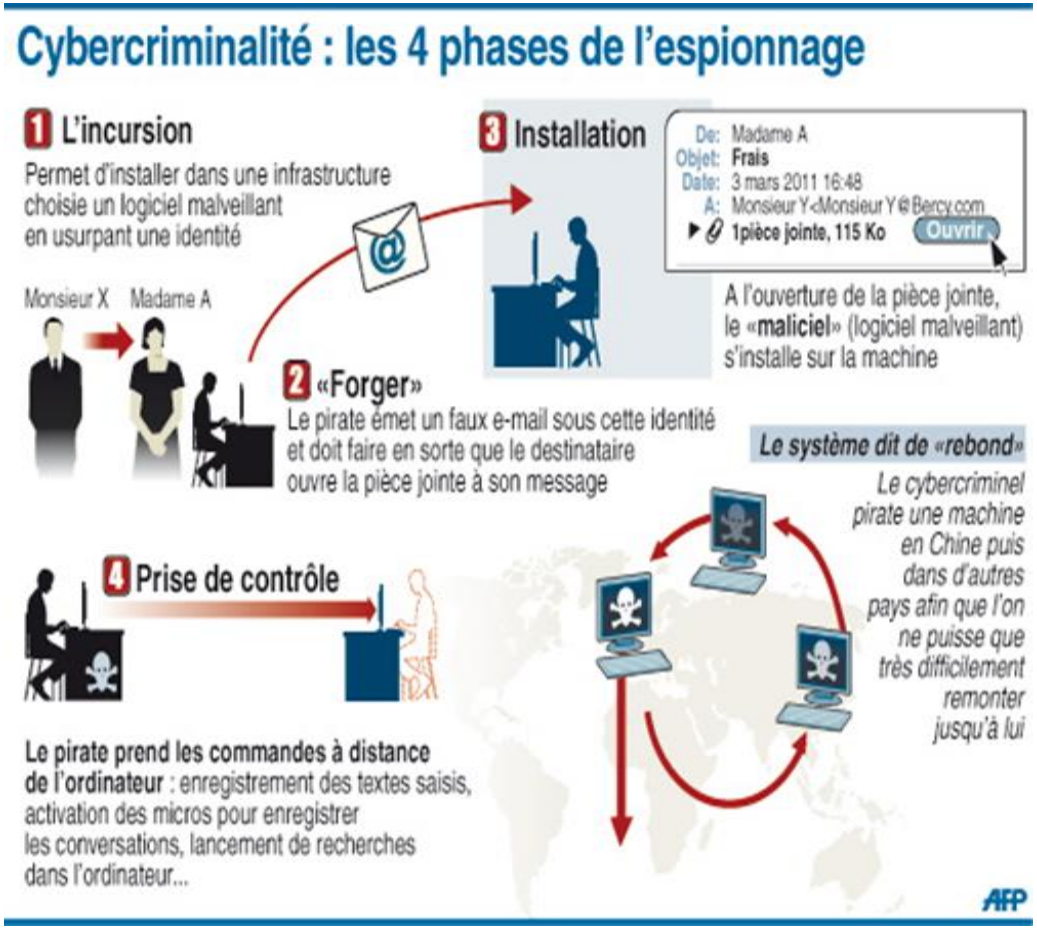
- Logiciel malveillant (ou malware) :
  - logiciel développé par un pirate dans le but de nuire à un système informatique : virus, ver, cheval de Troie.
  - Comment peut-il être transmis ?
    - par un réseau local ou internet ;
    - par un support contaminé (clé USB, disque dur externe…).

- Les pirates peuvent avoir plusieurs profils différents selon les actions menées : criminel, hacktiviste, initié (Ex : Edward Snowden).

Les attaques informatiques (cyberattaques)

- Les motivations des attaques peuvent être de différentes sortes :
  - obtenir un accès au système ;
  - voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
  - glaner des informations personnelles sur un utilisateur ;
  - récupérer des données bancaires ;
  - s'informer sur une organisation (entreprise de l'utilisateur, etc.) ;
  - troubler le bon fonctionnement d'un service ;
  - utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
  - utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

Les attaques informatiques : cybercriminalité



Les attaques informatiques : le défacement

- Un défacement (ou une défiguration) est la conséquence d'une faille de sécurité sur un site web. La page d'accueil est alors modifiée par les hackers.

- A quoi ressemble une page défacée ?
  - la page, généralement la page d'accueil,
    est un fond uni, souvent blanc ou noir ;
  - plusieurs éléments peuvent apparaitre sur cette page :
    - le pseudo du hacker, les mots « owned » ou « hacked » ;
    - une image qui affiche les revendications du pirate. On retrouve fréquemment des symboles (crâne ou drapeau) ;
    - la méthode utilisée pour hacker et défacer le site.
  - plusieurs phrases peuvent faire écho aux revendications du défaceur : contre le gouvernement, contre des défaceurs adverses, etc.

Les attaques informatiques : le «typosquatting»

- Le « typosquatting » consiste en l'acquisition de noms de domaine ressemblant de près à ceux de sites massivement consultés et à mettre à profit les similitudes ou les coquilles des internautes pour les rediriger vers des sites Web frauduleux.

- Le typosquatting est surtout utilisé pour récupérer les identifiants des visiteurs d'un site, mais il peut aussi être mis en place à des fins commerciales ou revendicatives.

Une arnaque aux faux billets Air France gratuits circule sur Internet

Des pirates du Net proposent sur Facebook, WhatsApp ou Snapchat des billets gratuits pour célébrer les 85 ans de la compagnie.

CYBERATTAQUE

ATTENTION, DES ANTI-VACCINS ONT RACHETE LE NOM DE DOMAINE «VITEMADOSE.FR»

Par CNEWS - Mis à jour le 11/05/2021 à 17:04
Publié le 11/05/2021 à 16:51

Les attaques : virus informatiques

- Un virus est un programme informatique qui s'insère dans le corps d'un autre programme en le parasitant (.exe) :
  - Le virus classique est un morceau de programme qui s'intègre dans un programme normal. Chaque fois que l'utilisateur exécute ce programme « infecté », il active le virus qui en profite pour aller s'intégrer dans d'autres programmes exécutables.
  - Le virus de boot s'installe dans un des secteurs de boot (contenant les éléments nécessaires au démarrage) d'un périphérique. Il remplace un chargeur d'amorçage (ou programme de démarrage ou « *bootloader* ») existant en copiant l'original ailleurs ;
  - Les macrovirus s'attaquent aux macros de logiciels de la suite Microsoft Office (Word, Excel, etc.). Par exemple, en s'intégrant dans le modèle normal.dot de Word, un virus peut être activé à chaque fois que l'utilisateur lance ce programme.

Les attaques : vers informatiques

- Le ver est un programme informatique qui se répand sur un réseau de façon autonome en exploitant des failles de logiciels (messagerie, ftp, etc.), ou des « failles utilisateur » :
  - Exemple: I love you est le nom d'un ver informatique, apparu pour la première fois le 4 mai 2000 et envoyé sous forme d'une pièce jointe à un courriel intitulé *I love you*. Le destinataire du courriel croit que la pièce jointe est un fichier de texte. En ouvrant le fichier, l'utilisateur déclenche l'exécution d'un programme contenu dans le fichier. Ce programme explore la liste des contacts de l'utilisateur et envoie à tous ses contacts un courriel contenant la pièce jointe infectée, assurant ainsi sa reproduction.

  - Il se reproduit et effectue la tâche pour laquelle on l'a programmé :
    - saturer les ressources disponibles ;
    - ralentir l'ordinateur et le réseau ;
    - détruire des données ou transférer des informations ;
    - espionner et offrir un point d'accès.

Les attaques : chevaux de Troie

- un peu d'histoire : après avoir vainement assiégé Troie pendant dix ans, les Grecs ont l'idée d'une ruse pour prendre la ville, construire un cheval géant en bois creux, dans lequel se cache un groupe de soldats. Un espion grec réussit à convaincre les Troyens d'accepter l'offrande. Le cheval est introduit dans l'enceinte de la cité. La nuit, lorsque les habitants sont endormis, les Grecs sortent du cheval et ouvrent les portes, permettant au reste de l'armée d'entrer et de piller la ville.
- un cheval de Troie est donc un logiciel apparemment inoffensif au sein duquel a été dissimulé un programme malveillant qui crée une porte cachée qui permet à son créateur d'entrer discrètement sur la machine infectée.
- il infecte la machine souvent suite à l'ouverture d'un fichier contaminé pour collecter des informations, voler des mots de passe, ouvrir une faille pour un pirate. Exemple : il peut permettre à un pirate d'utiliser votre PC comme serveur ou de récupérer vos coordonnées bancaires..

Les attaques : chevaux de Troie

- Appelés aussi RATS (Remote Administration Tools)

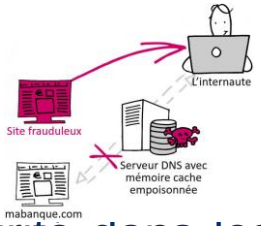
- C'est le type de virus le plus courant actuellement. Avec le cheval de Troie « Zeus », des cybercriminels ont dérobé 70 millions de dollars dans 190 pays. Ce cheval de Troie récupérait les informations bancaires saisies sur les ordinateurs pour transférer des fonds aux commanditaires.

- Le rançongiciel (ou *ransomware*) est un type de cheval de Troie qui connait la plus forte progression. Dissimulé dans une image ou un fichier téléchargé ou en exploitant les failles de sécurité de Internet Explorer, Flash player ou Java, il infecte l'ordinateur pour en chiffrer le contenu. Il devient alors impossible de lire les données stockées sur le disque dur. Pour récupérer ses fichiers, la victime n'a pas d'autre choix que de payer une rançon de plusieurs centaines d'euros.

Les attaques informatiques

- Autres attaques :
  - le pourriel (*spam* en anglais) : un courrier électronique non sollicité, la plupart du temps de la publicité ;
  - l'hameçonnage (*phishing* en anglais) : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles ;
  - le canular informatique (*hoax* en anglais) : un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes.
  - Le smishing : Le SMiShing (mot-valise composé de SMS et phishing) est une technique en plein essor qui fait appel aux messages des cellulaires (SMS) pour tromper des victimes en les incitant à agir immédiatement.

Les attaques informatiques



- Autres attaques (*suite*) :
  - L'injection SQL : il s'agit de l'exploitation d'une faille de sécurité dans les systèmes de bases de données relationnelles qui se réfèrent au langage SQL, un langage de programmation permettant de manipuler les bases de données.
    - En utilisant de manière ciblée les caractères de fonction, un utilisateur non autorisé peut s'infiltrer dans les commandes SQL et manipuler les saisies : changer des données, les supprimer ou les lire.
  - L'attaque par force brute (*bruteforce attack*) consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin de se connecter au service ciblé. Il s'agit d'une méthode courante chez les pirates.
  - Le DNS Cache Poisoning : L'empoisonnement du cache DNS ou « pollution de cache DNS » est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse.

Les attaques informatiques

- Les formes d'ingénierie sociale (manipulations psychologiques)

  – Arnaque au faux support technique : consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique et de payer des frais de « dépannage ». Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

  – L'escroquerie aux faux ordres de virement (FOVI) : désigne un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié. Parfois présenté comme émanant d'un dirigeant et ayant un caractère « urgent et confidentiel », on parle alors « d'arnaque au Président ».

Les attaques : actions à éviter

Quelles sont les actions à éviter ?

- De nombreuses pratiques peuvent exposer au risque d'une attaque informatique :
  - Ouvrir une pièce jointe en PDF ;
  - Brancher une clé USB reçue en cadeau ou « goodies » ;
  - Télécharger un film en pair à pair ;
  - Retarder les mises à jour des logiciels de sécurité de l'ordinateur ;
  - Etc.

- Des sites permettent de détecter une fuite potentielle de données personnelles : Have I been Pwned, Hacked emails.

Sommaire

- Les réseaux
- Les attaques
- Les mouchards (Spywares)
- La protection de la machine
- Les précautions à prendre

Les mouchards (spywares)

- Un logiciel espion ou espiogiciel espionne les habitudes de l'internaute dans le but de pouvoir cibler la publicité qui lui est proposée sur le web :
  - Ils sont souvent inclus dans des logiciels gratuits et s'installent généralement à l'insu de l'utilisateur ;
  - Ils infectent la machine lors de l'installation d'un gratuiciel ou partagiciel ;
  - Ils collectent les informations des utilisateurs ;
  - Ils transmettent les données via interne ;
  - Ils provoquent un ralentissement de l'ordinateur.

Sommaire

- Les réseaux
- Les attaques
- Les mouchards (Spywares)
- La protection de la machine
- Les précautions à prendre

La protection de la machine

- Règles élémentaires :
  - mettre régulièrement à jour ses logiciels, dont l'antivirus ;
  - ne pas télécharger de logiciels dont vous n'êtes pas sûr ;
  - ne pas ouvrir de fichiers exécutables (.exe, .scr) sans avoir la certitude qu'ils sont sains ;
  - ne pas ouvrir de fichiers joints à un mail sans avoir la certitude de leur origine ;
  - supprimer les mails provenant d'expéditeurs douteux ;
  - ne pas communiquer son adresse email sur des forums, blogs ou sites web ;
  - être attentif aux comportements anormaux de la machine : lenteur inhabituelle au démarrage, blocage de l'affichage, du réseau…

La protection de la machine

- Définir un mot de passe au démarrage de la machine :
  - permet à chaque utilisateur de protéger son espace de travail ;
  - le mot de passe doit être suffisamment long (8 caractères minimum) et mélanger différents types de caractères ;
    - il est impératif de ne pas utiliser ses nom et prénom, ceux de ses enfants ou toute autre information vous concernant (lieu de vacances ainsi que les mots de tous les dictionnaires français mais aussi étrangers.)
- Il est impératif de varier les mots de passe pour éviter le piratage en cas de fuite des données ;
- Installer les logiciels nécessaires à la protection de la machine :
  - antivirus ;
  - parefeu (firewall).

La protection de la machine : l'antivirus

- Un antivirus :
  - est un logiciel conçu pour protéger les ordinateurs des logiciels malveillants ;
  - possède une base de données de signatures virales ;
  - scanne les fichiers à la recherche de cette signature dans leur code.

- Trois fonctionnalités :
  - protection résidente ;
  - scanner ;
  - module de mise à jour des signatures virales.

La protection de la machine : l'antivirus

Si l'antivirus détecte une signature de virus connu, en fonction de la stratégie adoptée par l'utilisateur :

- il désinfecte le fichier et supprime le virus. S'il le peut ;
  - il met le fichier en quarantaine ;
  - il supprime le fichier ;
  - ou il le répare.

Principaux antivirus :

- Pour Windows
  - Kasperski, Bitdefender, Avira, F-Secure, Symantec Norton, Trend Micro, AVG antivirus, Avast Free, etc.
- Pour OS X
  - Symante Norton, Bitdefender, Kasperski, Avast gratuit pour Mac, Avira Free Antivirus pour Mac
- Pour Android
  - Gdata pour Android, Sophos Mobile, Trend Micro Mobile, Kasperski for Android, Avira Free Android

Le parefeu ou firewall

- Le parefeu :
  - il permet de protéger l'ordinateur des intrusions extérieures par le réseau internet :
    - vol de données par des pirates ;
    - installation de logiciels pouvant prendre le contrôle de la machine.
  - il agit comme un filtre entre le réseau et l'ordinateur.

- L'utilisateur définit la politique de sécurité du parefeu (blocages, autorisations).

Attention : ne pas confondre parefeu et anti-virus.
Le parefeu n'est pas suffisant pour vous protéger contre les virus.

Sommaire

- Les réseaux
- Les attaques
- Les mouchards (Spywares)
- La protection de la machine
- Les précautions à prendre

Les précautions à prendre

Attention aux réseaux Wi-Fi publics !

Sur un réseau Wi-Fi non sécurisé, un pirate peut voir le trafic de données et saisir l'occasion pour installer un logiciel malveillant sur votre terminal et/ou intercepter certaines de vos données.

Il est donc conseillé d'/de:

- Utiliser ce type de connexions et de réseaux seulement en cas d'urgence ;
- Eviter de s'y connecter si la connexion demande de fournir trop d'informations personnelles en échange ;
- Eviter de partager des données personnelles ;
- Ne pas rester connecté au Wi-Fi en permanence, la fonction Wi-Fi doit être désactivée lorsque celle-ci n'est pas utilisée (Ex : mode avion la nuit).
- Mettre à jour régulièrement le système d'exploitation et les pilotes Wi-Fi pour bénéficier d'une sécurité optimale.

Certaines bornes publiques ne donnent accès à Internet qu'après authentification sur un « portail captif » et permettent de bénéficier d'une connexion cryptée pour une meilleure sécurité. Exemple : eduroam.

Les précautions à prendre

Pour s’assurer que la connexion soit bien sécurisée :

- Vérifier le cadenas qui assure, entre autres, un paiement sécurisé ;

- Vérifier la mention HTTPS ;
- Se méfier des sites inconnus ou frauduleux qui imitent les sites légitimes ;
- Activer la double authentification ;
- Ne pas sauvegarder des données bancaires dans le navigateur.

A noter : Pour vérifier qu'un fichier n'a pas été modifié, il est possible de calculer sa "somme de contrôle" (procédé couramment utilisé en informatique pour vérifier l'intégrité de données) avec un algorithme particulier (exemples : SHA-256, SHA-512 ou SHA-3).

DSIUN – Service des usages numériques

- **Conception – Réalisation**
  - Alexa Gallo – Catherine Loire – Mélanie Mauvoisin - Service des usages numériques - Université Paris 1 Panthéon-Sorbonne
- **Sources**
  - Patricia Cavallo
  - Martine Fontaine

Version du support : 2.0
Septembre 2021

UNIVERSITÉ PARIS 1

PANTHÉON SORBONNE