

Sécurisation d'un réseau local

RÉALISÉ PAR :

Imane ZEROUALI

Abdousamad MOUSSA ELM

Mohamed El Mehdi TIOUICHI

M2 MATIS-SIRES
2016/2017



Plan

Introduction

1- Les menaces

- Définition

- Dangers encourus

- Degré d'intensité

2- Les techniques d'attaques

- les acteurs

- Scénario d'attaque

- Outils et types d'attaques

3- La sécurisation

- Services et garanties nécessaires

- L'authentification

- La confidentialité

Conclusion



Les menaces

1- Les menaces

Définition

Dangers encourus
Degré d'intensité

- 2- les techniques d'attaques
- 3- La sécurisation

- **Les garanties exigées**

- l'authentification
- la confidentialité
- l'intégrité
- la disponibilité

Pour assurer le niveau de garantie offert par le système d'information, des analyses peuvent être effectuées. Elles vont permettre d'évaluer le niveau de menace

Les menaces

1- Les menaces

Définition

Dangers encourus

Degré d'intensité

2- les techniques d'attaques

3- La sécurisation

Les actions adoptées le sont ensuite en toute connaissance de cause.

Le risque évalué peut être :

- Assumé
- Évité
- Limité
- Transféré

L'analyse et l'évaluation des risques permettent ainsi d'adopter des niveaux de sécurité appropriés, en fonction des garanties souhaitées pour le système d'information

Les menaces

1- Les menaces

Définition

Dangers encourus

Degré d'intensité

2- les techniques d'attaques

3- La sécurisation

DANGERS ENCOURUS

- RISQUES SUR LA CIRCULATION DES DONNEES.
- RISQUES AU NIVEAU DES PROTOCOLES RESEAU ET TRANSPORT.
- RISQUES AU NIVEAU DES PROTOCOLES APPLICATIONS STANDARD.
- RISQUE AU NIVEAU DES PROTOCOLES DE CAUCHES BASSES.
- RIQUES AU NIVEAU LOGICIEL.

Les menaces

1- Les menaces

Définition

Dangers encourus

Degré d'intensité

2- les techniques d'attaques

3- La sécurisation

LE DEGRES D'INTENSITE DE LA MENACE.

En complément de l'identification des cibles à protéger, et de leur vulnérabilités, une prise en compte des niveaux de menace permet d'affiner l'analyse.

Trois niveaux sont ainsi répertoriés :

- L'écoute ;
- L'intrusion ;
- La prise de contrôle.

Les menaces

1- Les menaces

Définition

Dangers encourus

Degré d'intensité

2- les techniques d'attaques

3- La sécurisation

LE DEGRES D'INTENSITE DE LA MENACE.

Ecoute des communications :

- L'écoute passive
- L'écoute active

Les menaces

1- Les menaces

Définition

Dangers encourus

Degré d'intensité

2- les techniques d'attaques

3- La sécurisation

LE DEGRES D'INTENSITE DE LA MENACE.

Intrusion et prise de contrôle :

Une intrusion est un accès illicite à un système. Le pirate accède ainsi à l'information elle-même ou aux services informatiques

RESUMER :

Nous pouvons comprendre que ces trois menaces ne présentent pas le même danger pour le réseau. Par contre, elle se complètent les unes par rapport aux autres, l'écoute facilitant l'intrusion, qui elle-même permet la prise de contrôle.

Les techniques d'attaques

1- Les menaces

2- les techniques d'attaques

Les acteurs

Scénario d'attaque

Outils et types d'attaques

3- La sécurisation

Une connaissance des agresseurs potentiels et de leurs capacités permet d'affiner le niveau de protection souhaitable.



Les techniques d'attaques

1- Les menaces

2- les techniques d'attaques

Les acteurs

Scénario d'attaque

Outils et types d'attaques

3- La sécurisation

•Employés de l'entreprise :



Les utilisateurs eux mêmes sont la cause d'un certain nombre d'incidents.

Risques :

- L'origine de l'exécution de code malveillants.
- Le non respect de la confidentialité des mots de passe

Précautions :

- Sensibilisation et information .

Les techniques d'attaques

1- Les menaces

2- les techniques d'attaques

Les acteurs

Scénario d'attaque

Outils et types d'attaques

3- La sécurisation

•Utilisateurs d'internet :



Nouvelles menaces pour l'entreprise sont venues avec la démocratisation de l'internet haut débit.

Risques :

- L'usage de logiciels pair à pair et de messageries électroniques facilite la promulgation des logiciels malveillants.
- La non mise à jour des signatures de virus et des correctifs de sécurité
- L'absence d'utilisation de pare-feu personnel

Exemple :

- Action de déni de service distribué (DDoS – Distributed Denial Of Service)

Précautions :

- sensibilisation et information aux dangers de l'internet.

Les techniques d'attaques

1- Les menaces

2- les techniques d'attaques

Les acteurs

Scénario d'attaque

Outils et types d'attaques

3- La sécurisation

•Acteurs expérimentés : (Hackers et Crackers)

- Des informaticiens qui connaissent très bien les systèmes et la programmation.
- Capable d'utiliser des techniques avancées.

•Acteurs inexpérimentés :

Qualificatifs :

- Newbies et Scripts Kiddies : En phase d'apprentissage, s'attaquent à des proies faciles .
- Lamer : Trouve ses ressources sur internet.



Les techniques d'attaques

1- Les menaces

2- les techniques d'attaques

Les acteurs

Scénario d'attaque

Outils et types d'attaques

3- La sécurisation

•Le scénario d'une attaque type :

- La recherche de renseignements
- La préparation
- L'intrusion
- L'installation
- Le camouflage
- La propagation



Les techniques d'attaques

1- Les menaces

2- les techniques d'attaques

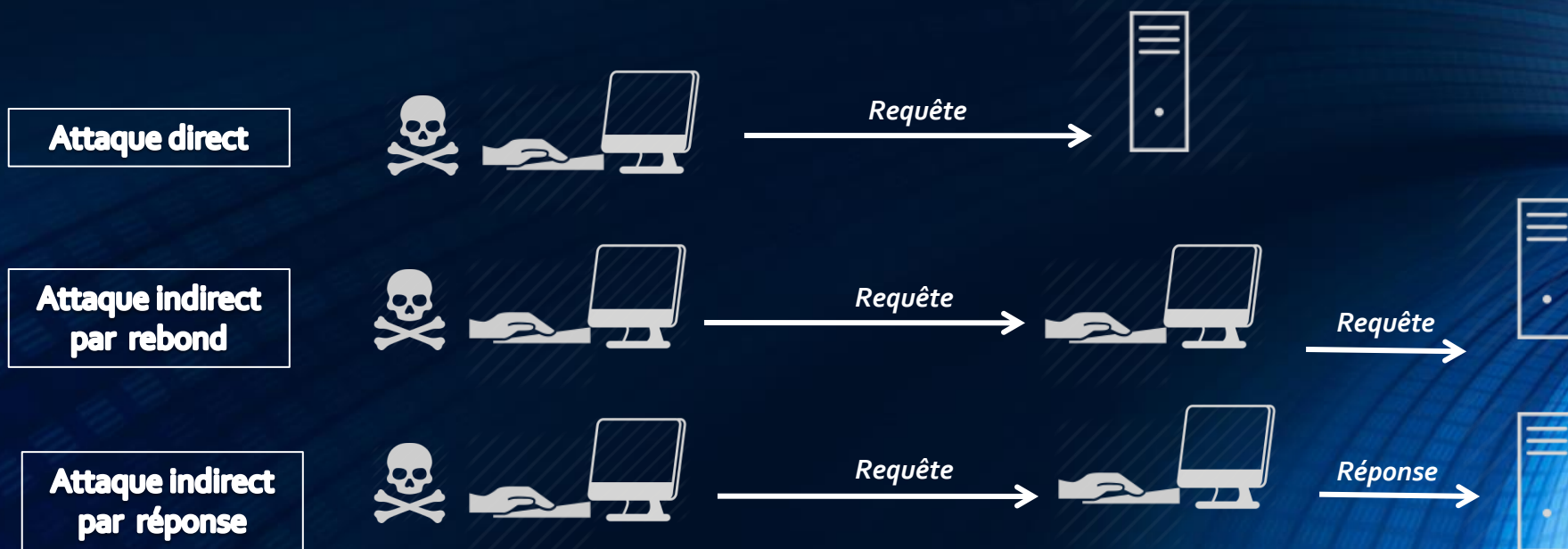
Les acteurs

Scénario d'attaque

Outils et types d'attaques

3- La sécurisation

•Outils et types d'attaques



3 familles d'attaques

Les techniques d'attaques

1- Les menaces

2- les techniques d'attaques

Les acteurs

Scénario d'attaque

Outils et types d'attaques

3- La sécurisation

•Les moyens de profiter les faiblesses d'un système :

Ingénierie sociale :

manipuler les personnes pour contourner les dispositifs de sécurité :
avoir les informations confidentielles par email
par téléphone

Écoute Réseau(sniffing) :

utiliser un analyseur de tram comme le logiciel libre
Ethereal

Analyse des ports :

utiliser un scanner des ports comme le logiciel
superscan et *NmapWin*

Code malveillant :

Virus
Ver (Worm)

Programmes furtifs :

Les logiciels d'espion : les programmes
keyloggers les bots, diminutif de robots
Plusieurs outils ont été conçues par Microsoft
pour lutter contre ces menaces comme le logiciel
ad-aware dont la version personnelle et gratuite

La sécurisation

1- Les menaces

2- les techniques d'attaques

3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité

Les différents services de sécurité à maintenir sont:

- Contrôles d'accès au système
- Gestion des habilitations
- Intégrités
- Non répudiation
- Authentification
- Confidentialité



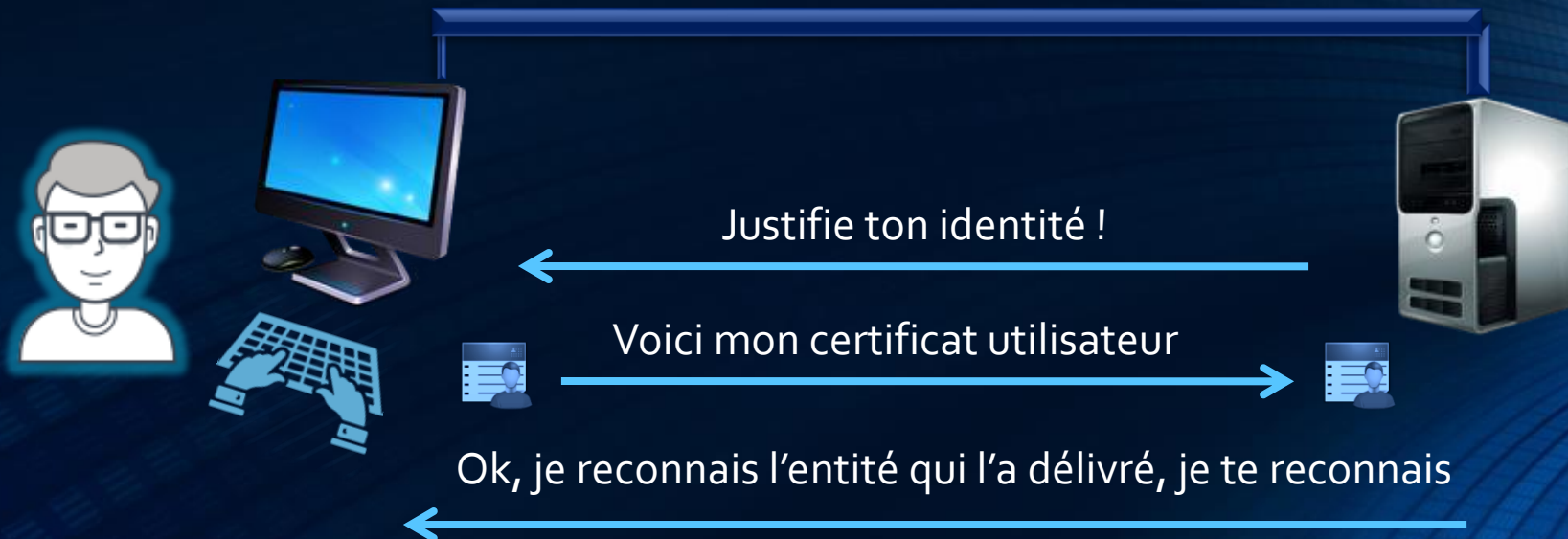
La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques
- 3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité



Processus d'identification

La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques
- 3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité

4 formes de vérification peuvent être exploitées:

- « Ce que je connais »
- « Ce que je possède »
- « Ce que je suis »
- « ce que je sais faire »



La sécurisation

1- Les menaces

2- les techniques d'attaques

3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité

Reconnaissance d'un certificat électronique:

- Un certificat est délivré par l'autorité de certification ou ses délégations.
- Elle doit être connue de l'ordinateur demandant la vérification.
- Elle est tiers de confiance.
- Les certificats peuvent justifier de l'identité d'un utilisateur ou d'un serveur.



La sécurisation

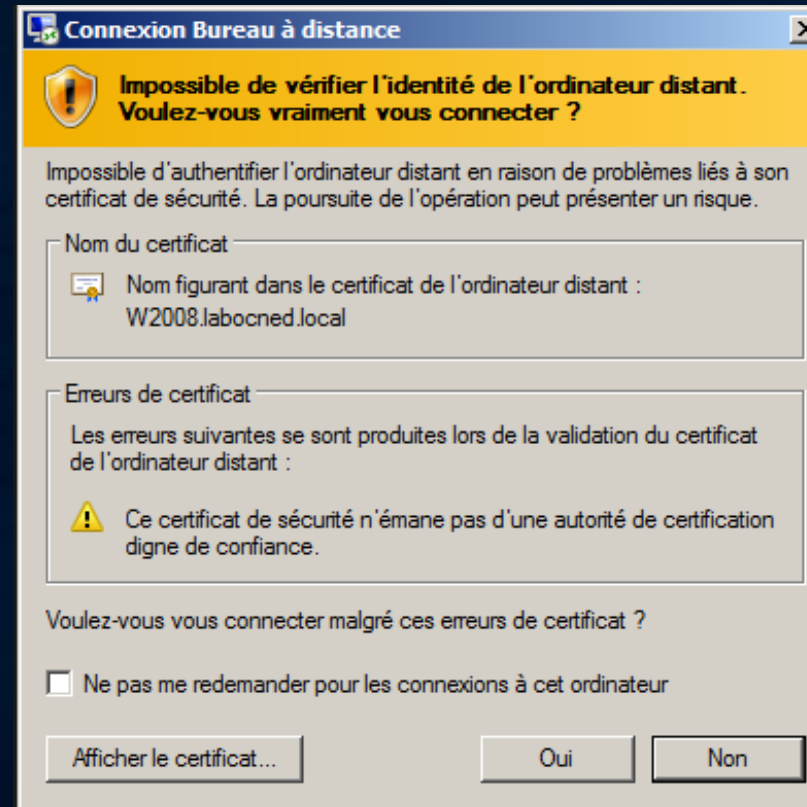
- 1- Les menaces
- 2- les techniques d'attaques

3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité



Message d'erreur indiquant la non reconnaissance de l'autorité de certification du certificat

Src: <http://docplayer.fr/4104828-Support-des-services-et-des-serveurs.html>

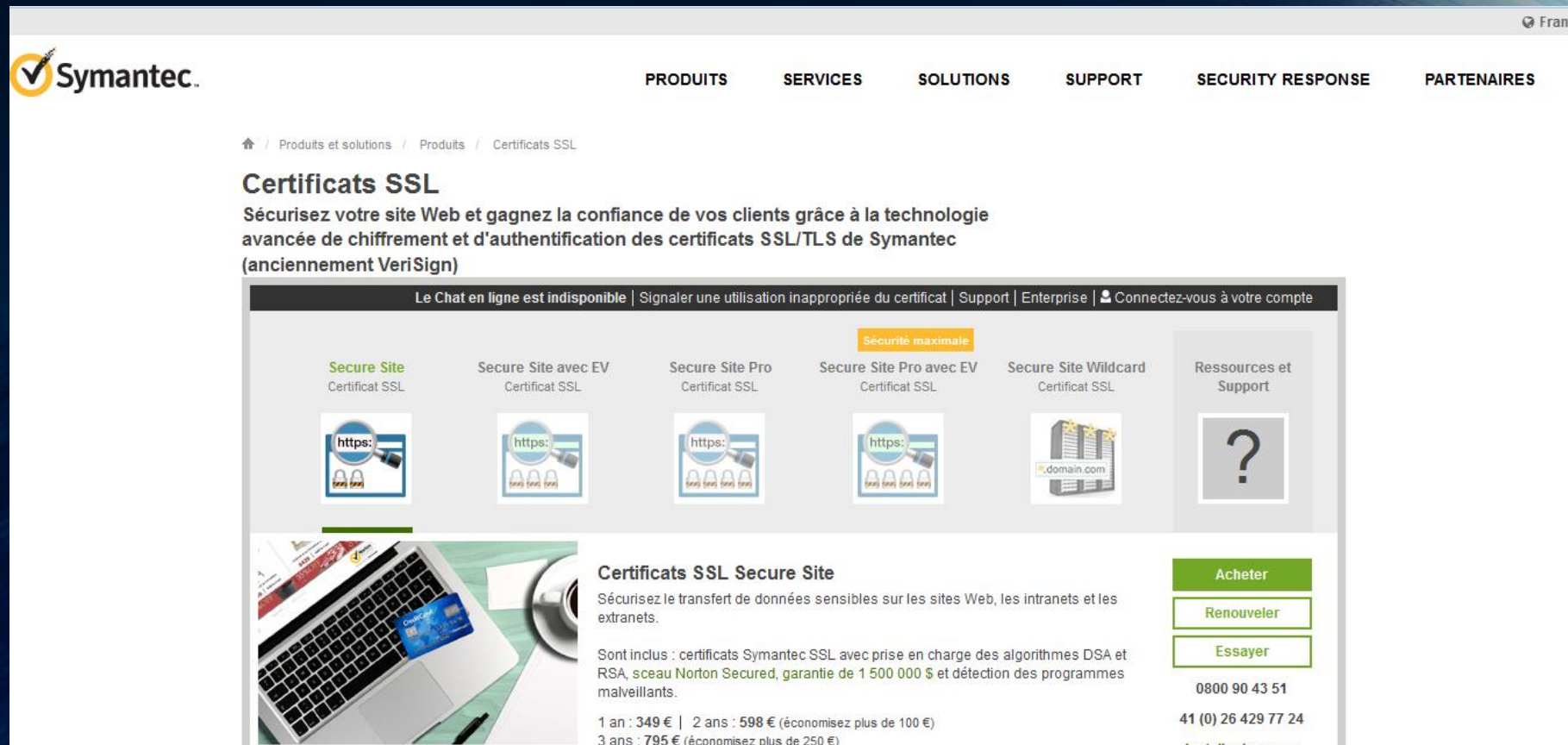
La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques
- 3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité



The screenshot displays the Symantec website's SSL certificate section. At the top, the Symantec logo is on the left, and navigation links for 'PRODUITS', 'SERVICES', 'SOLUTIONS', 'SUPPORT', 'SECURITY RESPONSE', and 'PARTENAIRES' are on the right. Below the navigation, a breadcrumb trail reads 'Produits et solutions / Produits / Certificats SSL'. The main heading is 'Certificats SSL', followed by a subheading: 'Sécurisez votre site Web et gagnez la confiance de vos clients grâce à la technologie avancée de chiffrement et d'authentification des certificats SSL/TLS de Symantec (anciennement VeriSign)'. A dark banner below the heading contains links: 'Le Chat en ligne est indisponible | Signaler une utilisation inappropriée du certificat | Support | Enterprise | Connectez-vous à votre compte'. The main content area features six product cards: 'Secure Site Certificat SSL', 'Secure Site avec EV Certificat SSL', 'Secure Site Pro Certificat SSL', 'Secure Site Pro avec EV Certificat SSL' (marked 'Sécurité maximale'), 'Secure Site Wildcard Certificat SSL', and 'Ressources et Support'. Each card has an icon representing the certificate type. Below the product cards, there is a detailed section for 'Certificats SSL Secure Site'. This section includes an image of a laptop with a credit card, a description: 'Sécurisez le transfert de données sensibles sur les sites Web, les intranets et les extranets.', and a list of included features: 'certificats Symantec SSL avec prise en charge des algorithmes DSA et RSA, sceau Norton Secured, garantie de 1 500 000 \$ et détection des programmes malveillants.' Pricing is listed as: '1 an : 349 € | 2 ans : 598 € (économisez plus de 100 €) | 3 ans : 795 € (économisez plus de 250 €)'. To the right of the pricing, there are three buttons: 'Acheter', 'Renouveler', and 'Essayer', followed by contact numbers '0800 90 43 51' and '41 (0) 26 429 77 24'.

Site web de la société SYMANTEC de délivrance des certificats

Src: <https://www.symantec.com>

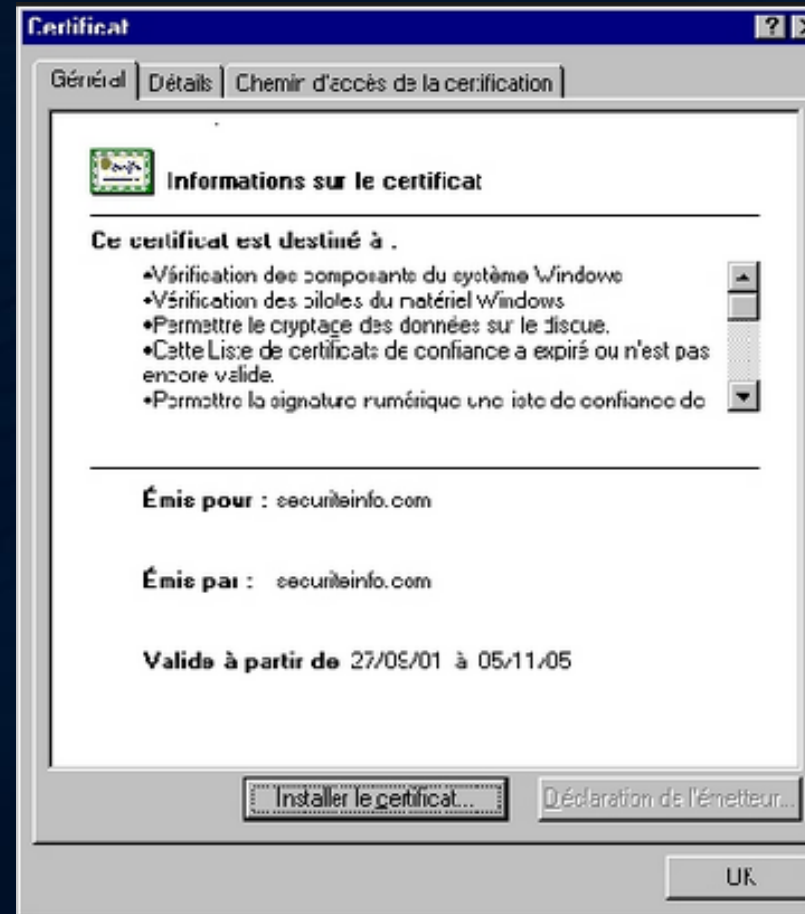
La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques
- 3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité



Exemple d'un Certificat

Src: <https://www.securiteinfo.com/cryptographie/pki.shtml>

La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques

3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité

Authentification à mot de passe :

- Statique.
- Dynamique:



RSA SecurID

Src: <https://www.rsa.com>

La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques
- 3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité

Authentification avec support physique:



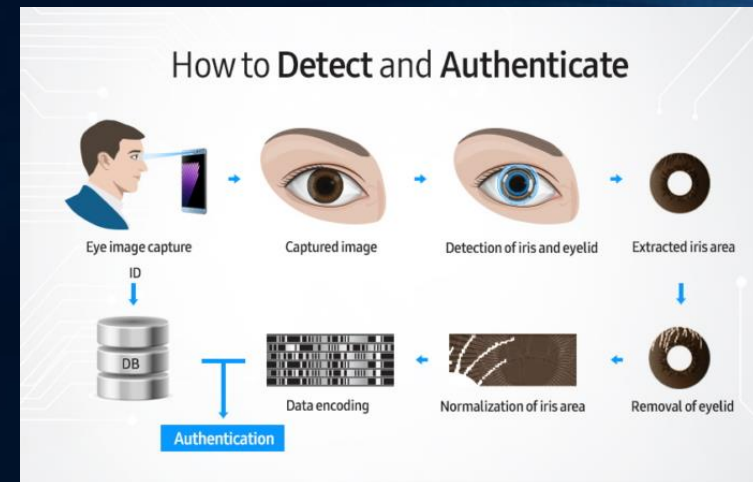
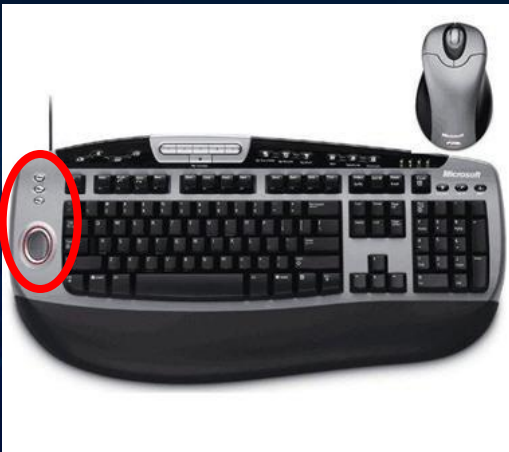
Src: <https://www.motorola.com/> Src : <http://gestion-des-temps.bodet-software.com/>

PUCE RFID: puce électronique sous la peau

La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques
- 3- La sécurisation
 - Services et garanties nécessaires
 - L'authentification
 - La confidentialité

Authentification à caractéristique humaines :



Src: <http://www.labibitteduweb.ca/tag/biometrie/>

La sécurisation

1- Les menaces

2- les techniques d'attaques

3- La sécurisation

Services et garanties nécessaires

L'authentification

La confidentialité

La confidentialité:

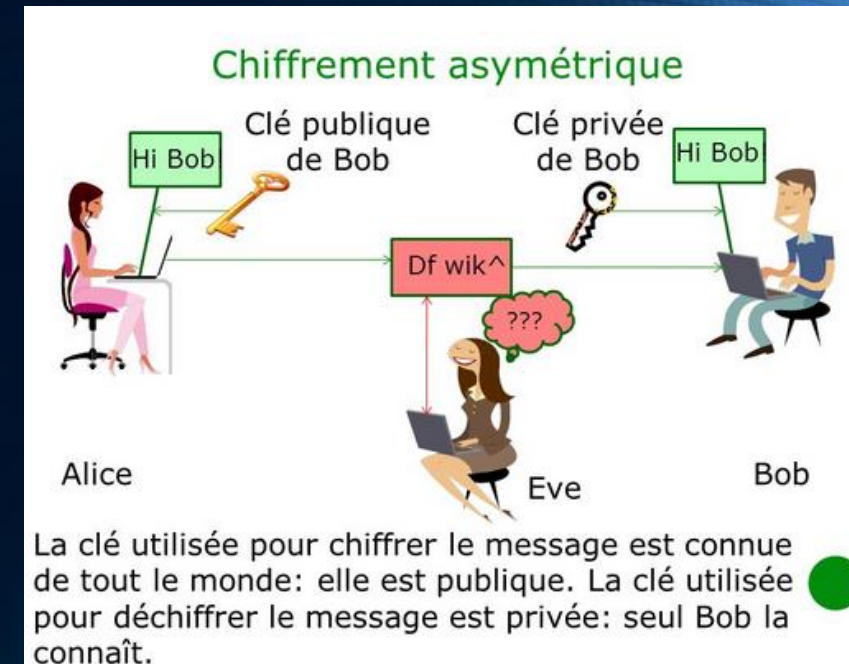
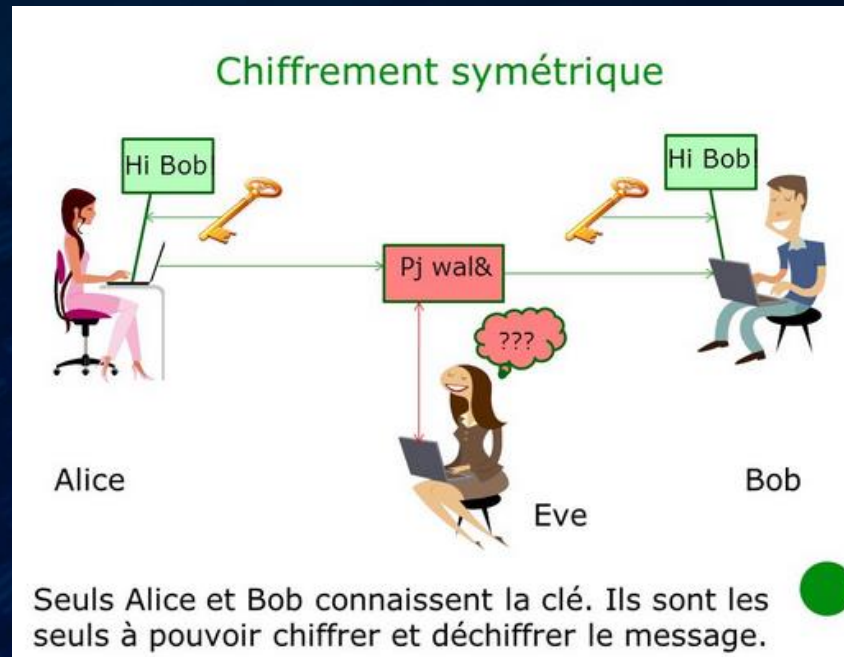
- Rendre secret un message à l'aide de la cryptographie.
- Cryptage à l'aide du chiffrement à clef(s).



La sécurisation

- 1- Les menaces
- 2- les techniques d'attaques
- 3- La sécurisation
 - Services et garanties nécessaires
 - L'authentification
 - La confidentialité

Deux famille de systèmes crypto pour rendre confidentiel des communication réseaux, la mise en ouvre:



Bibliographie

Livres et sites web

Src: www.mi.parisdescartes.fr/~mea/cours/Mi/Mi.1.pdf

Src: <http://docplayer.fr/4104828-Support-des-services-et-des-serveurs.html>

Src: <https://www.symantec.com>

Src: <https://www.securiteinfo.com/cryptographie/pki.shtml>

Src: <https://www.rsa.com>

Src: <https://www.motorola.com/>

Src : <http://gestion-des-temps.bodet-software.com>

Src: <http://www.labibitteduweb.ca/tag/biometrie/>

Src: <http://securit.free.fr>

Merci de votre
attention

