Table of contents

Introduction

Les Services de Sécurité Fondamentaux

Les services de sécurité sont les objectifs que l'on cherche à atteindre pour protéger un système.

- **Confidentialité** : Protection contre la divulgation non autorisée.
- **Intégrité** : Protection contre la modification non autorisée.
- **Disponibilité** : Garantie d'accès pour les utilisateurs légitimes.
- **Authentification** :
  - *Entity authentication* (Entité) : Certifier l'identité d'un acteur.
  - *Data origin authentication* (Origine) : Certifier la source d'une donnée.
- **Non-répudiation** : Impossibilité de nier une transaction.
- **Non-Duplication** : Protection contre les copies illicites.
- **Anonymat** : Préservation de l'identité ou de la source.

Version originale

- **Confidentialité** : Protection de l'information d'une divulgation non autorisée.
- **Intégrité** : Protection contre la modification non autorisée de l'information.
- **Disponibilité** : S'assurer que les ressources sont accessibles aux utilisateurs légitimes.
- **Authentification** :
  - **Authentification d'entités** *(entity authentication)* : procédé permettant à une entité d'être sûre de l'identité d'une seconde entité à l'appui d'une évidence corroborant (p.ex.: présence physique, cryptographique, biométrique, etc.). Le terme identification est parfois utilisé pour désigner également ce service.
  - **Authentification de l'origine de données** *(data origin authentication)* : procédé permettant à une entité d'être sûre qu'une deuxième entité est la source originale d'un ensemble de données. Par définition, ce service assure également l'intégrité de ces données.
- **Non-répudiation** : Offre la garantie qu'une entité ne pourra pas nier être impliquée dans une transaction.
- **Non-Duplication** : Protection contre les copies illicites.

- **Anonymat (d'entité ou d'origine de données)** : Permet de préserver l'identité d'une entité, de la source d'une information ou d'une transaction.

Synthèse : Services, Menaces et Mécanismes de Protection

Services de Sécurité	Dangers et Attaques (*Italique*)	Mécanismes Classiques	Mécanismes Digitaux
Confidentialité	Fuite d'informations, *eavesdropping* (écoutes), analyse du trafic	Scellés, coffre-forts, cadenas	Cryptage, autorisation logique
Intégrité	Modification, *tampering* (altération), création ou destruction illicite	Encre spéciale, hologrammes	Fonctions à sens unique + cryptage
Disponibilité	*Denial of Service (DoS)*, virus, usage illicite	Contrôle d'accès physique, surveillance vidéo	Contrôle d'accès logique, audit, anti-virus
Authentification d'entités	Accès non autorisés, vol de mot de passe, faille de protocole	Présence, voix, pièce d'identité, biométrie	Secret + protocole, adresse réseau + userid, carte à puce + PIN
Authentification de données	Falsification d'informations ou de signature	Sceaux, signature, empreinte digitale	Fonctions à sens unique + cryptage
Non-répudiation	Nier une transaction (*repudiation*), prétendre un vol de clé	Sceaux, signature notariale, envoi recommandé	Fonctions à sens unique + cryptage + signature digitale
Non-duplication	Duplication, falsification, imitation	Encre spéciale, hologrammes, tatouage	Tatouage digital (*watermarks*), verrouillage cryptographique
Anonymat	Identification, analyse de transaction, traçage	Brouilleur de voix, déguisement, argent liquide	*Mixers*, *remailers*, argent électronique, *deep web*

Version originale

Dangers et Attaques : Synthèse

Services	Dangers	Attaques
Confidentialité	fuite d'informations	écoutes illicites, analyse du trafic
Intégrité	modification de l'information	création, altération ou destruction illicite
Disponibilité	denial of service, usage illicite	virus, accès répétés visant à inutiliser un système
Authentification d'entités	accès non autorisés	Vol de mot de passe, faille dans le protocole d'authentification
Authentification de données	falsification d'informations	falsification de signature, faille dans le protocole d'authentification
Non-répudiation	nier la participation à une transaction	prétendre un vol de clé ou une faille dans le protocole de signature
Non-duplication	duplication	falsification, imitation
Anonymat	identification	analyse d'une transaction, accès non autorisés permettant l'identification

Mécanismes de Protection

Services	Mécanismes classiques	Mécanismes digitaux
Confidentialité	scellés, coffre-forts, cadenas	cryptage, autorisation logique
Intégrité	encre spéciale, hologrammes	fonctions à sens unique + cryptage
Disponibilité	contrôle d'accès physique, surveillance vidéo	contrôle d'accès logique, audit, anti-virus
Auth. d'entités	présence, voix, pièce d'identité, reconnaissance biométrique	secret + protocole d'authentification, adresse réseau + userid, carte à puce + PIN
Auth. de données	sceaux, signature, empreinte digitale	fonctions à sens unique + cryptage
Non-répudiation	sceaux, signature, signature notariale, envoi recommandé	fonctions à sens unique + cryptage + signature digitale
Non-duplication	encre spéciale, hologrammes, tatouage	tatouage digital (watermarks), verrouillage cryptographique
Anonymat	brouilleur de voix, déguisement, argent liquide	mixers, remailers, argent électronique, deep web

---

Risques Liés à Internet

Programmes Malveillants Transmis par E-Mail

- Aussi appelés **maliciels** (*malware*).
- E-mails visant à **provoquer une action** (ouvrir une pièce jointe ou cliquer sur un lien).
- Attaques souvent **personnalisées** grâce à l'**ingénierie sociale**.
- **Conséquences principales :**
  - Installation de malware (*ransomware*, *keyloggers*, etc.).
  - **Perte ou vol de données** personnelles.
  - **Détournement du système** et **propagation** du malware.

Ultra-synthèse

- Malware diffusé par e-mail
- Incitation à cliquer ou ouvrir
- Ingénierie sociale
- Vol, perte de données, détournement

Version originale

Programmes Malveillants Transmis par E-Mail

- Aussi appelés **maliciels** ou *malware*.
- E-mails conçus pour **inciter le destinataire** à **ouvrir une pièce jointe** ou à **suivre un lien** contenant de la publicité non souhaitée, des informations offensives, des programmes à risque, etc.
- Souvent ciblés sur la base des intérêts de la victime (travail préliminaire d'ingénierie sociale (*social engineering*)).
- **Conséquences :**
  - Installation de malware (*ransomware*, *keyloggers*, etc.) dans le système de la victime (*ordinateur*, *tablette*, *smartphone*, *smartwatch*, etc.).
  - Destruction de données contenues dans l'ordinateur.
  - Vol d'informations ou de données personnelles.
  - Détournement du système pour des fins malicieuses (p.ex.: minage illicite de *bitcoins*).
  - Diffusion de *malware* (éventuellement à d'autres utilisateurs).

Programmes Malveillants Transmis sur le Web

- Méthode appelée ***drive-by download*** : **infection automatique lors de la visite d'un site web**.
- L'origine peut être :
  - un **site malveillant** ;
  - un **site légitime compromis** (p. ex. *cross-site scripting*).
- La **prudence des utilisateurs** limite fortement ce mode de propagation.
- Les **impacts sont similaires** aux infections par e-mail.
- La **restriction des scripts** (*java/javascript*) réduit les risques mais peut **affecter la navigation**.

Ultra-synthèse

- *Drive-by download* = infection sans action de l'utilisateur
- Sites malveillants ou compromis
- Sensibilisation + scripts restreints = protection

Version originale

Programmes Malveillants Transmis sur le Web

- Cette technique, souvent appelée ***drive-by download***, permet d'**infecter le système** (*ordinateur*, *tablette*, *smartphone*, *smartwatch*, etc.) **sur lequel s'exécute un client web lors de la simple visite d'un site**.
- Il peut s'agir soit :
  - d'un site malicieux qui contient le *malware*.
  - d'un site web légitime qui aurait été infecté au préalable (par exemple, moyennant une technique appelée *cross-site scripting*). L'infection pouvant affecter seulement certaines pages…
- La sensibilisation des utilisateurs (ne pas visiter des sites douteux) diminue l'efficacité de cette technique dans la transmission de *malware*.
- Les conséquences sont semblables à celle des transmissions par e-mail.
- L'exécution restreinte des scripts (*java/javascript*) dans le navigateur peut limiter la portée de l'infection mais risque de contraindre la navigation dans certains sites.

Hameçonnage (Phishing)

- Technique visant à **collecter des informations privées** par des méthodes de **pêche indiscriminée**.
- Le ***phishing*** peut être :
  - **général** (ciblage large) ;
  - **ciblé** (*spear phishing*) lorsqu'une personne ou organisation précise est visée.
- Le vecteur principal est un **e-mail à adresse falsifiée**, difficilement détectable.
- L'objectif est d'obtenir des **données sensibles** (identifiants, mots de passe, informations personnelles ou bancaires).
- Les attaques reposent sur des **prétextes crédibles ou menaçants** pour pousser la victime à coopérer.

Ultra-synthèse

- Vol d'informations par tromperie
- E-mails falsifiés
- *Spear phishing* = attaque ciblée
- Prétextes urgents ou menaçants

Version originale

Hameçonnage (Phishing)

- Le mot ***phishing*** se compose des mots anglais ***"password"*** (mot de passe), ***"harvesting"*** (moisson) et ***"fishing"*** (pêche).
- Cette composition de mots illustre le but principal de cette technique qui consiste à **récolter un maximum d'informations privées** des utilisateurs via des mécanismes de "pêche indiscriminée".
- Lorsque la pêche aux informations est ciblée vers une personne ou organisation spécifique, la technique est dénommée ***spear phishing*** (qui provient de *spear fishing* ou pêche au harpon).
- Le vecteur de transmission consiste normalement dans un e-mail avec une **adresse d'expédition falsifiée** (mais souvent indétectable…) qui demande à la victime de fournir des informations privées : adresses e-mail, identifiants (*twitter*, *facebook*, etc.), mots de passe, numéros d'identité, numéros de comptes bancaires, etc.
- Les prétextes utilisés sont variés (mise à jour du système informatique, arrêt du service, retrait d'un envoi, etc.) et vont jusqu'à menacer l'utilisateur en cas de refus.

Pourriels (Spam)

- E-mails **indésirables**, souvent publicitaires, ou **pop-ups** non sollicités lors de la navigation web.
- Représentent environ **60% des e-mails mondiaux**.
- Conséquences principales :
  - **Consommation de ressources** et perte de temps.
  - Certains peuvent **transmettre des malware**.
- Ciblent souvent les adresses courtes ou proviennent de **listes d'adresses vendues/échangées**.
- Les **filtres anti-spam** entraînent des **coûts importants** pour les organisations.

Ultra-synthèse

- E-mails/publicités indésirables
- Risques : perte de temps, ressources, malware
- Ciblage : adresses courtes ou listes
- Filtrage coûteux pour entreprises

Version originale

Pourriels (Spam)

- Englobe tous les **e-mails indésirables** (souvent publicitaires) reçus par les personnes et les organisations.
- Terme utilisé également pour désigner les **pages/*fenêtres pop-up* affichées sans le consentement de l'utilisateur** lors de la navigation web.
- On estime que **60%** des e-mails qui circulent dans le monde appartiennent à cette catégorie.
- Les conséquences sont souvent limitées à la consommation de ressources de calcul et stockage ainsi qu'au gaspillage de temps associé à la lecture et traitement de ces messages mais…
- … **certains e-mails spam** peuvent également constituer des **vecteurs de transmission de malware**.
- Ils ont tendance à cibler plus particulièrement les adresses e-mail courtes (p.ex: abc@gmail.com) mais fonctionnent également sur la base des listes (souvent échangées / vendues) contenant tous types d'adresses.
- Les opérations de **filtrage anti-spam** entraînent des coûts considérables pour les organisations.

Rançongiciels (Ransomware)

- Malware type **Cheval de Troie** qui **chiffre les données** pour les rendre inaccessibles.
- Exige une **rançon** (souvent en bitcoins) pour récupérer les fichiers.
- Peut rester **dormant**, déclenché par un événement ou une date.
- Principal vecteur : **e-mails malveillants**.
- Autres effets possibles : **attaques par déni de service, extorsion**.

Ultra-synthèse

- Chiffrement des données par Cheval de Troie
- Rançon pour restaurer accès
- Dormance programmée possible

- Infection via e-mails malveillants

Version originale

Rançongiciels (Ransomware)

- Cette famille spécifique de malware appartient à la catégorie appelée **Chevaux de Troie** (Trojan Horses).
- Leur comportement plus habituel consiste à **chiffrer les données de la victime** (locaux et distants) **afin de les rendre totalement inaccessibles**.
- Un message apparait ensuite pour demander le paiement d'une rançon (souvent en **bitcoins** ou une autre monnaie virtuelle) permettant potentiellement de récupérer l'accès aux fichiers chiffrés.
- Ils peuvent rester en ***état dormant*** dans le système infecté et être déclenchés par un événement spécifique ou à une date donnée (attaques synchronisées).
- Leurs vecteurs d'infection sont variés mais les **e-mails contenant des pièces jointes malicieuses** sont souvent mis en cause lors des infections primaires.
- Des nombreuses variantes existent et continuent à se développer.
- On observe parfois d'autres comportements associés à ces *malware* : **dénis de service**, **extorsions ciblées**, **menaces**, etc.

Attaques sur les Dispositifs *Internet of Things (IoT)*

- Attaques visant les **objets connectés** (caméras, TV, capteurs, alarmes, etc.).
- Ces dispositifs sont **faciles à compromettre** à cause de :
  - **failles connues**,
  - **mots de passe par défaut**,
  - **manque de sensibilisation** des utilisateurs.
- La **prise de contrôle à distance** permet :
  - un **point d'entrée** vers le réseau,
  - l'**utilisation de l'appareil** pour des activités illicites (DDoS, hacking, minage).
- Un **inventaire précis** des dispositifs connectés est indispensable.

Ultra-synthèse

- Cible les objets connectés
- Sécurité faible (failles, mots de passe par défaut)
- Risque d'accès au réseau et d'abus
- Inventaire des IoT nécessaire

Version originale

Attaques sur les Dispositifs *Internet of Things (IoT)*

- Ciblent les **objets connectés** de toute sorte (caméras, TVs, frigos, capteurs et interrupteurs domotiques, installations d'alarme, etc.).
- Ils sont souvent **plus faciles à pirater** que les systèmes traditionnels par cause de :
  - nombreuses failles de sécurité souvent connues des attaquants.
  - mots de passe par défaut.
  - négligence de la part des utilisateurs qui ignorent les risques qui leurs sont propres.
- La **prise de contrôle à distance** de ces appareils par une entité malveillante implique :
  - Une porte d'entrée au réseau domestique/corporatif.
  - Un dispositif pouvant être utilisé pour des activités illicites (hacking, attaques DDoS, minage de bitcoins, etc.).
- L'établissement d'un répertoire précis de tous les dispositifs de ce type connectés au réseau est nécessaire!

Modification Illicite des Informations Publiées (*Information Spoofing and Website Defacement*)

- Attaques visant à **altérer les informations** sur sites web et réseaux sociaux.
- Impact : **réputation compromise** et **dommages économiques**.
- Sites web : sécurisation du système hôte, configuration restrictive, **audits réguliers**.
- Réseaux sociaux : mots de passe forts, **authentification multi-facteur**, fermeture des sessions, suppression des *cookies*.

Ultra-synthèse

- Altération des infos sur sites et réseaux sociaux
- Risques : réputation et pertes économiques
- Sites : sécurisation + audits
- Réseaux sociaux : mots de passe forts, MFA, sessions fermées, cookies supprimés

Version originale

Modification Illicite des Informations Publiées (*Information Spoofing and Website Defacement*)

- Attaques visant **l'intégrité** de l'information publiée dans les sites web, les réseaux sociaux, etc.
- Elles portent atteinte à la **réputation** et peuvent provoquer d'importants **dommages économiques** pour les sociétés ayant une présence Internet.
- Dans le cas des **sites web**, la **sécurisation du système hôte** est essentielle ainsi qu'une **configuration aussi restrictive que possible**. Des audits des sécurité récurrents sont vivement recommandés.
- La **protection des informations affichées dans les réseaux sociaux** dépend directement du processus d'authentification permettant d'accéder au profil à risque :
  - Éviter les mots de passe trop simples.
  - Privilégier l'authentification forte, si possible *multi-facteur*.
  - Fermer proprement les sessions.
  - Effacer les *cookies*.

Attaques Dénis de Service (*Denial of Service / DDoS*)

- Vise à **rendre inaccessibles des systèmes informatiques**, surtout pour les organisations.
- **DDoS** : attaque distribuée par des milliers de dispositifs, générant un trafic massif.
- Protections classiques (*firewalls*, sondes IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)) souvent **insuffisantes**.
- Conséquences :
  - **Réputation affectée**
  - **Pertes financières** (parfois rançons)
  - **Risques élevés** pour les infrastructures critiques (hôpitaux, centrales, Internet backbone)

Ultra-synthèse

- DDoS = systèmes inaccessibles via attaques massives
- Protections limitées
- Risques : réputation, finances, infrastructures critiques

Version originale

Attaques Dénis de Service (*Denial of Service* / *DDoS*)

- Attaques destinées à **rendre inaccessibles des systèmes informatiques** de toute sorte visant surtout les organisations privées ou étatiques.
- Le terme **DDoS** (*Distributed Denial of Service*) désigne une famille d'attaques dans laquelle des multiples (**souvent des dizaines de milliers) de dispositifs ciblent simultanément le(s) système(s) victime(s)**.
- Le trafique généré atteint plusieurs centaines de gigabits / seconde.
- L'efficacité des mécanismes de protection traditionnels (*firewalls*, *sondes* de *prévention* et de *détection d'intrusion*, etc.) est limitée.
- L'indisponibilité d'un service peut engendrer :
  - des problèmes **réputationnels**.
  - d'importantes **pertes financières** (des **demandes de rançon** peuvent être exigées pour les désactiver).
  - des **hauts risques de sécurité (même physique!)** lorsque des **infrastructures critiques** (hôpitaux, centrales électriques, *backbone* de l'Internet, etc.) sont ciblées.

Méthodes Digitales de Sécurité

Problème : Protéger des informations digitales

- dans un environnement distribué
- globalement accessible
- sans frontière matérielle

Solution :

- Cryptographie
  - Symétrique
  - Asymétrique
  - + fonctions à sens unique
  - + générateurs (pseudo) aléatoires

Ultra-synthèse

- **Problème** : Sécurité dans un environnement distribué/global.
- **Solutions** :
  - Crypto (symétrique/asymétrique).
  - Fonctions à sens unique (hachage).
  - Générateurs aléatoires (physiques/pseudo).

Version originale

Problème : Protéger des informations digitales

- dans un environnement distribué
- globalement accessible
- sans frontière matérielle

Solution :

- Cryptographie
  - Symétrique
  - Asymétrique
  - + fonctions à sens unique
  - + générateurs (pseudo) aléatoires

Fonctions de Hachage Cryptographiques

- **Fonctions faciles à calculer dans un sens mais virtuellement impossibles à inverser**.
- Toute modification du document source change radicalement le **digest** (effet avalanche).
- **Propriétés clés** :
  - **One-way** : impossible de retrouver l'entrée depuis le hash.
  - **Collision-free** : impossible de trouver deux entrées avec le même hash.
- Taille des digests : 160 à 512 bits.
- Algorithmes (très **performants**) : SHA-1, SHA-256, SHA-3.

Ultra-synthèse

- **One-way + collision-free**.
- Taille : 160-512 bits.
- Algos : SHA-1/256/3.
- Usage : intégrité, signatures.

Version originale

- **Fonctions faciles à calculer dans un sens mais virtuellement impossibles à calculer dans le sens contraire**.

- Toute modification (même insignifiante) du document source se traduit par un **digest** fondamentalement différent.
- Il est virtuellement impossible de retrouver le document source à l'aide seulement du digest (**one-way**).
- Il est virtuellement impossible de retrouver un deuxième document source produisant le même digest (**collision-free**).
- Longueur habituelle des digests : 160 à 512 bits.
- Les algorithmes à sens unique sont très performants.
- Exemples : SHA-1, SHA-256, SHA-3, etc.

Générateurs (Pseudo) Aléatoires

- **Caractéristiques**
  - **aléatoire**
  - **imprévisible**
  - **non reproductible**
- **Critique** pour la sécurité (clés, IV, secrets).
- **Types** :
  - **Vrais aléatoires** : basés sur phénomènes physiques (radioactivité, quantique).
  - **Pseudo-aléatoires** : déterministes (basés sur un *seed*: séquence aléatoire initiale).
- **Risque** : "Pseudo-sécurité" si le *seed* est prévisible (citation de Pitkin).
- Applications : clés de session, IV (DES-CBC), signatures (ElGamal).

Ultra-synthèse

- **Vrais aléatoires** : physiques (quantique).
- **Pseudo-aléatoires** : déterministes (*seed*).
- **Risque** : *seed* prévisible = faille.
- Usages : clés, IV, signatures.

Version originale

- La génération de nombre aléatoire est un processus très important pouvant compromettre la sécurité d'un bon nombre de systèmes de cryptage.
- Applications : génération de clés de session, vecteurs d'initialisation (DES - CBC mode), secrets pour signatures (ElGamal), etc.

- Un **générateur aléatoire** (random generator) est un dispositif capable de générer des nombres de façon **aléatoire**, **imprévisible** et **non reproductible**. (e.g. basé sur phénomènes physiques: source radioactive ou quantique).
- Les **générateurs pseudo-aléatoires** sont des procédés déterministes développés à partir d'une séquence aléatoire initiale (**seed**) (e.g. frappe utilisateur, accès disque).
- *Citation :* R. Pitkin dans [Kau95]: "The use of pseudo-random processes to generate secret quantities can result in pseudo-security"

Cryptographie Symétrique

- **Historique** : Utilisée depuis Jules César (I av. J.-C.).
- **Principe** : Une seule clé pour chiffrer/déchiffrer.
- **Schéma** : Plaintext → Cryptage (Clé) → Ciphertext → Décryptage (Clé) → Plaintext.
- **Caractéristiques** :
  - Algorithmes : AES, DES, IDEA, RC4.
  - Services : Confidentialité, Authentification, Intégrité.
  - **Limite** : Pas de signatures (clé partagée).
  - **Problème** : Échange de clé sécurisé requis.

Ultra-synthèse

- **1 clé** pour chiffrer/déchiffrer.
- **Rapide** (AES, DES).
- **Problème** : échange de clé.
- Usages : documents personnels, groupes fermés.

Version originale

- Aussi appelée cryptographie conventionnelle ou à clés secrètes (I av. JC, Julius Cesar).
- **Idée :** Sur la base d'une seule clé secrète, réaliser une transformation capable respectivement de rendre illisible et de restituer une pièce d'information.
- **Schéma :** Plaintext → Cryptage (Clé) → Ciphertext → Décryptage (Clé) → Plaintext.
- **Caractéristiques :**
  - Algorithmes : AES, DES, IDEA, RC4, RC5, etc. (certains sont gratuits et de libre accès)

- Services : Confidentialité, Authentification, Intégrité.
- Pas de support direct pour signatures digitales (car clé connue des deux).
- Nécessite un canal confidentiel pour échanger la clé.
- Idéal pour la protection de documents personnels ou groupes fermés.

Cryptographie Asymétrique

- Aussi appelée **cryptographie publique** (1976, Diffie & Hellman).
- **Principe**
  - Paire de clés (publique/privée) pour chiffrement et signatures.
- **Deux usages principaux** :
  1. **Confidentialité** :
     - Chiffrement : clé publique du destinataire
     - Déchiffrement : clé privée du destinataire
  2. **Signature numérique** :
     - Signature : clé privée de l'expéditeur
     - Vérification : clé publique de l'expéditeur
     - *Optimisation* : On signe généralement le **hash** du document
     - **Propriétés fondamentales** :
       * **Intégrité** : Toute modification invalide la signature
       * **Non-collision** : Impossible d'avoir 2 documents avec la même signature
       * **Non-répudiation** : Seul le détenteur de la clé privée peut signer
- **Aspects techniques** :
  - **Algorithmes** : RSA, ElGamal
  - **Services** : Intégrité, Authentification, Non-Répudiation
  - **Performance** : beaucoup plus lent que le symétrique (100x plus lent)
  - **Avantage** : Pas besoin de canal confidentiel pour l'échange de clés

Ultra-synthèse

- **2 clés** : publique (chiffrer/vérifier) + privée (déchiffrer/signer)
- **2 usages** :
  - Confidentialité : chiffrer pour un destinataire
  - Signature : prouver l'authenticité
- **Signatures** :

  - Intégrité + non-répudiation

- **Algorithmes** : RSA/ElGamal
- **Avantage** : Pas besoin de canal sécurisé pour échanger les clés
- **Désavantage** : Lente

Version originale

Cryptographie Asymétrique

- Aussi appelée cryptographie publique ou à clés publiques (1976, W. Diffie & M. Hellman).
- **Idée :** Utiliser deux clés différentes - une **secrète** et une **publique** - respectivement pour les opérations de cryptage et décryptage.
- Chaque utilisateur dispose d'un **porte-clés** (keyring).

Confidentialité : * Expéditeur crypte avec la **clé publique du destinataire**. * Destinataire décrypte avec sa **clé privée**. * Uniquement clé du destinataire utilisée ! **Signature Digitale :** * Expéditeur signe avec sa **clé privée**. * Destinataire vérifie avec la **clé publique de l'expéditeur**. * Uniquement clé de l'expéditeur utilisée ! * *Note :* On signe généralement le **digest** du document (hash) pour des raisons de performance. **Caractéristiques des signatures :** * La signature change si le document change, alors que la clé privée reste la même. * En cas de modification du document ou de la signature, la vérification échoue (**intégrité garantie**). * Il est virtuellement impossible, même pour le détenteur de la clé privée, de générer un second document produisant la même signature (fonction à sens unique **sans collisions**). * Seul le détenteur de la clé privée peut générer une signature vérifiable à l'aide de la clé publique correspondante (**non-répudiation**). * **Algorithmes** : RSA, ElGamal. * **Services** : Intégrité, Authentification, Non-Répudiation. * **Lenteur** : Jusqu'à 50 fois plus lent que la cryptographie symétrique. * **Avantage** : Pas besoin de canal confidentiel pour échanger les clés (contrairement au symétrique).

Crypto Asymétrique + Symétrique (Hybride)

- **Principe** : Utiliser l'asymétrique pour échanger une clé symétrique (clé de session).
- **Étapes** :

  1. A génère une clé symétrique aléatoire K_s.
  2. A chiffre K_s avec la clé publique de B.
  3. A et B communiquent ensuite avec K_s (symétrique).

Ultra-synthèse

- **Asymétrique** : échange de clé symétrique.
- **Symétrique** : chiffrement des données.
- **Avantage** : combine sécurité + performance.

Version originale

- **Idée :** Utiliser la cryptographie publique uniquement pour échanger des clés symétriques (Clés de session).
- A génère une clé aléatoire K_s et la transmet à B en l'encryptant avec la clé publique de B.
- A & B communiquent ensuite en utilisant K_s (symétrique).

Cryptographie Asymétrique : Fonctionnement (RSA)

Construction des clés

1. **Choix des nombres premiers** :
   - p et q : deux grands nombres premiers (> 1024 bits)
   - $n = pq$: module RSA (taille = 2048+ bits)
2. **Calcul de l'indicatrice d'Euler** :
   - $\phi(n) = (p-1)(q-1)$
   - *Propriété* : Pour tout a premier avec n, $a^{\phi(n)} \equiv 1 \pmod{n}$
3. **Sélection des exposants** :
   - e : entier premier avec $\phi(n)$ (exposant public)
   - d : inverse modulaire de e (exposant privé), tel que $ed \equiv 1 \pmod{\phi(n)}$

Processus de chiffrement/déchiffrement

- **Clé publique** : (n, e)
- **Clé privée** : (d)
- **Chiffrement** : $C = P^e \pmod{n}$
- **Déchiffrement** : $P = C^d \pmod{n}$

Preuve mathématique

1. **Congruence fondamentale** :
   - $ed = 1 + k\phi(n)$ (par définition de d)
2. **Application du théorème d'Euler** :
   - $P^{\phi(n)} \equiv 1 \pmod{n}$ (si P premier avec n)
3. **Démonstration** :

$$\begin{aligned}(P^e)^d &\equiv P^{ed} \pmod{n} \\ &\equiv P^{1+k\phi(n)} \pmod{n} \\ &\equiv P \cdot (P^{\phi(n)})^k \pmod{n} \\ &\equiv P \cdot 1^k \pmod{n} \\ &\equiv P \pmod{n}\end{aligned}$$

Sécurité du système

- **Problème difficile** : Factorisation de n en p et q
- **Taille recommandée** :
  - n : 2048 bits (minimum pour sécurité actuelle)
  - p et q : 1024+ bits chacun
- **Vulnérabilités connues** :
  - Attaques par canal auxiliaire (timing, power analysis)
  - Choix inapproprié des paramètres (e trop petit, p et q trop proches)

Ultra-synthèse

- **Clés** :
  - Publique : (n, e) où $n = pq$
  - Privée : (d) avec $ed \equiv 1 \pmod{\phi(n)}$
- **Opérations** :
  - Chiffrement : $P^e \mod n$
  - Déchiffrement : $C^d \mod n$
- **Sécurité** : Factorisation de n difficile
- **Taille** : 2048+ bits pour n

Version originale

Cryptographie Asymétrique: Fonctionnement (RSA)

- Soit $n := pq$ avec p et q deux nombres premiers grands (> 1024 bits).
- Soit $\phi(n) = (p-1)(q-1)$.
- Soit e et d tels que $ed \equiv 1 \pmod{\phi(n)}$.
- Par définition des congruences: $ed = 1 + k\phi(n)$
- Théorème d'Euler : $a^{\phi(n)} \equiv 1 \pmod{n}$.
- **Encryption :** $C = P^e \pmod{n}$. **Clé publique :** (n, e).
- **Décryption :** $P = C^d \pmod{n}$. **Clé privée :** (d).
- *Preuve :* $(P^e)^d \equiv P^{ed} \equiv P^{1+k\phi(n)} \equiv (P \pmod{n})(P^{\phi(n)} \pmod{n})^k \equiv P \pmod{n}$.

Cryptographie Asymétrique : Conclusions

- **Algorithmes dominants** : RSA (le plus utilisé), Rabin, ElGamal
- **Services complets** :
  - Confidentialité
  - Authentification
  - Intégrité
  - Signature digitale & Non-répudiation
  - Non-duplication
- **Performances** :
  - 50x plus lent que le symétrique
  - **Solution optimale** : Combinaison asymétrique (échange de clés) + symétrique (chiffrement)
- **Gestion des clés** :
  - **Avantage** : Échange de clés publiques sans canal confidentiel
  - **Risque** : Nécessité de vérifier l'authenticité des clés publiques
    - Canal d'acquisition authentifié **ou**
    - Certification par tiers de confiance

Ultra-synthèse

- **Algos** : RSA (dominant), Rabin, ElGamal
- **Services** : Confidentialité + Authentification + Intégrité + Signatures
- **Lenteur** : 50x vs symétrique → **hybride recommandé**

- **Clés** : Échange public simple mais **authentification cruciale**

Version originale

Cryptographie Asymétrique : Conclusions

- Il existe quelques systèmes de cryptage asymétrique (**Rabin**, **ElGamal**, etc.) mais le plus utilisé est **RSA**.
- **Services supportés** : **Confidentialité**, **Authentification**, **Intégrité**, **Signature Digitale & Non-Refus**, (**Non Duplication**).
- Les opérations liées à la **cryptographie asymétrique** sont jusqu'à **50 fois (!) plus lentes** que celles de la **cryptographie symétrique**. Une **combinaison des deux méthodes** est souvent souhaitable.
- La **distribution des clés** est simplifiée par le fait que seules des **clés publiques** doivent être échangées entre les intervenants (pas besoin d'un canal confidentiel alternatif) mais…
- … il est nécessaire de **vérifier que la clé publique appartient réellement au destinataire** :
  - Soit le **canal d'acquisition** de la clé publique est protégé contre toute modification (**authentifié**)
  - Soit la clé est **certifiée exacte par un tiers**

Comparaison Symétrique vs Asymétrique

Avantages comparés

- **Symétrique** :
  - **Performance** : 100x plus rapide
  - **Implémentation** : Facile en hardware
  - **Clés** : Courtes (128 bits = 16 caractères mémorisables)
- **Asymétrique** :
  - **Échange de clés** : Canal authentifié suffisant (pas besoin de confidentialité)
  - **Gestion** : 1 paire de clés pour n correspondants (vs n clés en symétrique)

Problématiques communes

- **Maillon faible** : Gestion des clés par les utilisateurs
- **Base de sécurité** : Empirique plutôt que théorique
- **Contraintes légales** : Restrictions d'usage et d'exportation

Recommandations d'usage

Cas d'usage	Solution recommandée	Justification
Documents personnels	Symétrique	Vitesse + clés mémorisables
Groupes d'utilisateurs proches	Symétrique	Vitesse + échange confidentiel facile
Utilisateurs distants/inconnus	Asymétrique	Pas besoin de canal confidentiel
Transactions distantes	Hybride (Asymétrique + Symétrique)	Asymétrique pour l'échange de clé, symétrique pour les données
Protection logicielle (distribution)	Hybride	Clé symétrique unique par version, encryptée avec asymétrique
Segments réseaux	Symétrique	Vitesse + environnement contrôlé (échange de clés facile entre administrateurs)

Ultra-synthèse

Symétrique :

```
Rapide (100x)
Clés courtes (128 bits)
Échange de clés confidentiel requis
```

Asymétrique :

```
Échange de clés simplifié
1 paire de clés pour n correspondants
Lent (50x)
Clés longues (1024+ bits)
```

Hybride : Meilleur des deux mondes **Problèmes communs** : Gestion des clés, base empirique, restrictions légales

Version originale

Cryptographie Symétrique vs. Asymétrique

- Il existe des **centaines d'algorithmes symétriques et asymétriques** capables de fournir un niveau de **confidentialité suffisant**.
- Les **solutions symétriques** offrent les avantages suivants :
  - **Rapidité** (jusqu'à **100 fois plus rapide** que les solutions asymétriques)
  - **Facilité d'implantation en hardware**
  - **Longueur de clé réduite** : **128 bits** (= 16 caractères mémorisable !) au lieu de **1024 bits** pour des équivalents asymétriques.
- Les **solutions asymétriques** ont comme arguments principaux :
  - **Échange de clés simplifié** : les clés doivent être échangées par un **canal authentifié mais non-confidentiel**
  - **Gestion de clés simplifiée** : une seule **paire de clés publique/privée** suffit à un utilisateur pour recevoir des messages confidentiels de **n utilisateurs** (au lieu de **n clés différentes** dans le cas symétrique).
- **Problèmes propres aux deux techniques** :
  - La **gestion de clés par l'utilisateur** reste le **maillon le plus faible**
  - Sécurité (normalement) basée sur des **arguments empiriques** plutôt que **théoriques**
  - **Restrictions légales** d'usage et d'exportation

Cryptographie Symétrique vs. Asymétrique (II)

Activité	Recommandation	Remarques
Protection de documents personnels	**Crypto symétrique**	**Vitesse**, clés facilement mémorisables
Protection de documents dans un groupe d'utilisateurs proches	**Crypto symétrique**	**Vitesse**, facilité d'échange des clés confidentielles
Établissement de canaux confidentiels entre utilisateurs distants (inconnus)	**Crypto asymétrique**	Pas besoin d'avoir un canal confidentiel : **authenticité suffit**
Transactions entre deux utilisateurs distants, Protection de logiciel (distribution multicast)	**Crypto asymétrique pour protection de clé symétrique + Crypto symétrique pour protection des données**	**Vitesse**, Seule la clé symétrique doit être ré-encryptée pour chaque correspondant, Copie cryptée du logiciel peut être rendue publique
Protection des segments réseaux	**Crypto symétrique**	**Vitesse**, Environnement stable → échange confidentiel des clés facile entre sysadmins

Dissection d'une Attaque : Ransomware

Définition et Impact

- **Définition** : Logiciel malveillant qui chiffre les données et exige une rançon pour leur restitution.
- **Limites de la définition classique** :
  - Ne couvre pas l'impact sur **l'infrastructure critique** (ex : Colonial Pipeline, mai 2021)
  - Sous-estime la **portée systémique** des attaques
- **Statistiques alarmantes** :
  - Milliards d'attaques annuelles
  - Considéré comme la **menace cyber la plus dangereuse** en 2021 ("Ransomware Everywhere")

Ultra-synthèse

- **Malware** : Chiffre les données → demande rançon
- **Impact** : Infrastructure critique (ex : Colonial Pipeline)

- **Menace n°1** en cybersécurité (2021)
- **Cibles** : Particuliers + entreprises + États

Version originale

"Un rançongiciel (de l'anglais **ransomware**), logiciel rançonneur, logiciel de rançon ou logiciel d'extorsion, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel **chiffre des données personnelles** puis demande à leur propriétaire d'envoyer de l'argent en échange de la **clé de déchiffrement**" (Wikipedia 21 septembre 2021).

- **Définition incomplète** car les **ransomwares** portent sur un **vaste spectre de l'infrastructure informatique**
- À titre d'exemple, en mai 2021, une **attaque ransomware** dirigée contre la société **Colonial Pipeline** a provoqué une **coupure d'approvisionnement** de combustible d'une grande partie de la côte des États-Unis
- Avec un nombre d'**attaques global** chiffré en **milliards par année**, "**Ransomware Everywhere**" est globalement considérée comme la **menace la plus directe, visible et dangereuse** pour utilisateurs et entreprises en 2021 !

Cycle de Vie d'une Attaque Ransomware

Prévention et Réponse

Phase	Mesures
Prévention	- Patching régulier- Solutions de détection (Firewalls, WAFs, IDS/IPS)- Scans anti-malware (e-mails, fichiers)
Protection	- **Backups offline** (essentiel !)- Politiques de sécurité strictes- Formation des utilisateurs
Réponse	- **Ne pas payer** (recommandation officielle)- Analyse forensique- Restauration depuis backups

Dissection Technique

1. **Infection** :

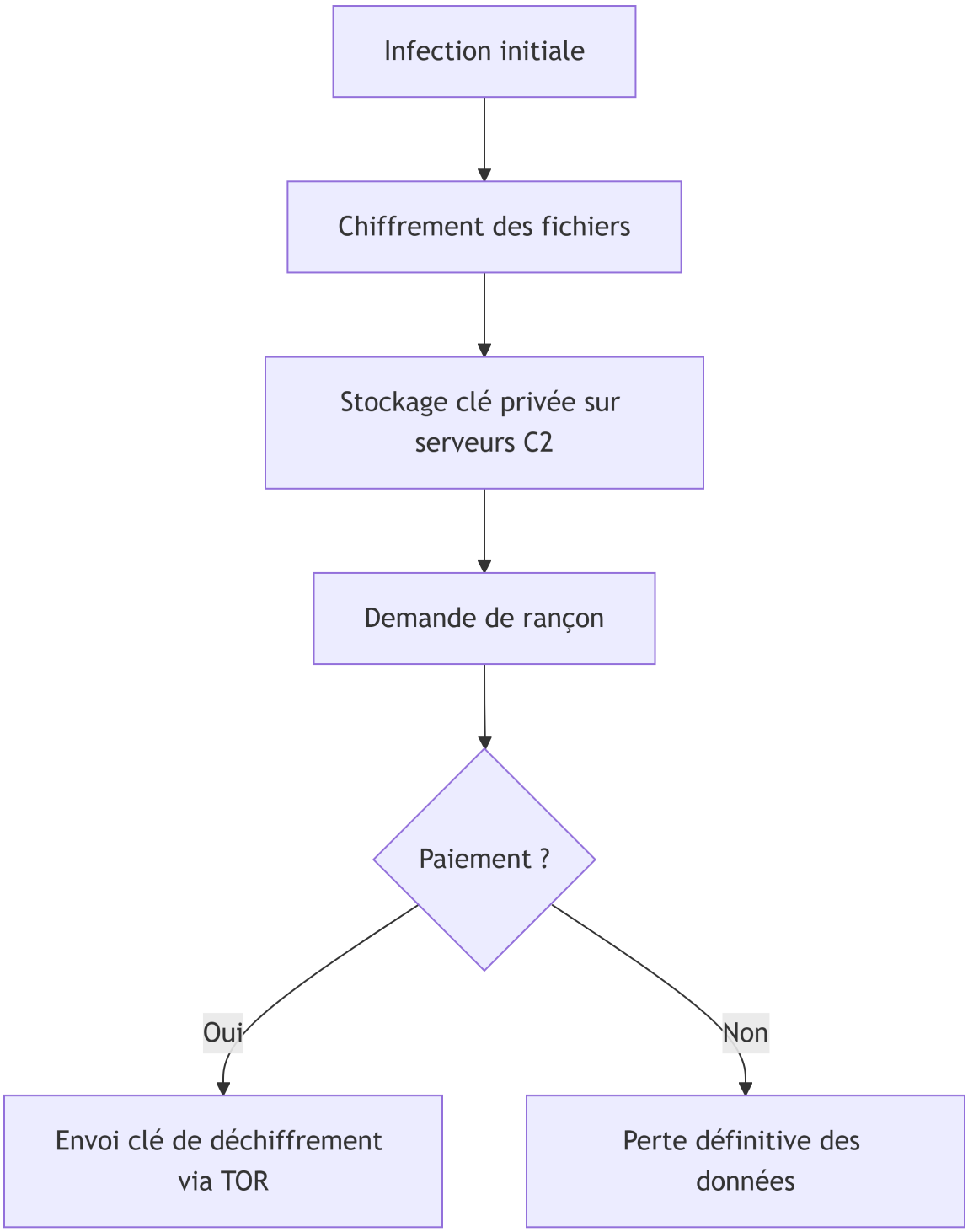
- Vecteurs : Phishing, exploits, RDP vulnérable
- Propagation : Latérale (réseau) ou verticale (système)

2. **Exécution** :
   - Chiffrement des fichiers ciblés
   - Suppression des shadow copies
   - Persistance (registre, tâches planifiées)
3. **Extorsion** :
   - Affichage de la demande de rançon
   - Paiement en cryptomonnaies (Bitcoin, Monero)
   - Délais de paiement avec majoration
4. **Occultation** :
   - Obfuscation du code
   - Communication via TOR/Deep Web
   - Effacement des logs

> **Ultra-synthèse**
>
> **Cycle d'attaque** :
>
> 1. Infection (phishing/exploits)
> 2. Exécution (chiffrement + persistance)
> 3. Extorsion (rançon en crypto)
> 4. Occultation (TOR + effacement traces)
>
> **Contre-mesures** :
>
> ```
> Backups offline
> Patching + détection
> Formation
> Ne pas payer
> ```

Cryptolocker : Analyse Technique

Schéma d'Attaque


Infection initiale
Chiffrement des fichiers
Stockage clé privée sur serveurs C2
Demande de rançon
Paiement ?
Oui
Non
Envoi clé de déchiffrement via TOR
Perte définitive des données

Cibles Privilégiées

- **Extensions critiques** (extrait) :
  - Documents : `.docx`, `.xlsx`, `.pdf`, `.pptx`
  - Bases de données : `.mdb`, `.sql`, `.sqlite`
  - Médias : `.jpg`, `.png`, `.mp4`, `.avi`
  - Développement : `.java`, `.cpp`, `.py`, `.php`
  - Financier : `.qbw`, `.qbb`, `.wallet`
- **Comportement** :
  - Chiffrement **sélectif** (fichiers récents/modifiés)
  - **Double extorsion** : Chiffrement + menace de fuite
  - **RaaS** (Ransomware-as-a-Service) : Modèle économique

Ultra-synthèse

Mécanisme : - Clé privée stockée sur serveurs C2 - Paiement → clé via TOR - Cibles : 100+ extensions (docs, DB, médias)
Évolutions récentes : - Double extorsion (chiffrement + fuite) - RaaS (location de ransomware)

Version originale

Ransomware : Vue Intégrale

(Source : 2017 State of Cybersecurity, F-Secure Inc.)

Ransomware : Vue Intégrale

Prévision, Remédiation et Réaction

- **Patching**
- **Détection active et passive** (Firewalls, WAFs, IDS, IPS, e-mail malware scan, etc.)
- **Backups offline** !
- **Politique de Sécurité** - Règles de bon usage de la messagerie
- **Formation** !
- **Payer ou pas payer…**

Dissection Technique de l'Attaque

- **Infection et propagation**
- **Exécution**

- **Paiement** (Crypto-currencies / Bitcoin)
- **Occultation** (Obfuscation, TOR Networks/Deep Web)

Schéma Générique d'un Ransomware Cryptolocker

- Les **clés privées de déchiffrement** sont stockées dans les serveurs de l'**attaquant**
- Elles sont envoyées à la **victime** après **paiement en bitcoins**
- La **trace** est broyée à l'aide des **réseaux TOR**

Ransomware Cryptolocker : Cibles

Extensions de fichiers ciblées : .jin, .xls, .xlsx, .pdf, .doc, .docx, .ppt, .pptx, .txt, .dwg, .bak, .bkf, .pst, .dbx, .zip, .rar, .mdb, .asp, .aspx, .html, .htm, .dbf, .3dm, .3ds, .3fr, .jar, .3g2, .xml, .png, .tif, .3gp, .java, .jpe, .jpeg, .jpg, .jsp, .php, .3pr, .7z, .ab4, .accdb, .accde, .accdr, .accdt, .ach, .kbx, .acr, .act, .adb, .ads, .agdl, .ai, .ait, .al, .apj, .arw, .asf, .asm, .asx, .avi, .awg, .back, .backup, .backupdb, .pbl, .bank, .bay, .bdb, .bgt, .bik, .bkp, .blend, .bpw, .c, .cdf, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfp, .cgm, .cib, .class, .cls, .cmt, .cpi, .cpp, .cr2, .craw, .crt, .crw, .phtml, .php5, .cs, .csh, .csl, .tib, .csv, .dac, .db, .db3, .dbjournal, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der, .des, .design, .dgc, .djvu, .dng, .dot, .docm, .dotm, .dotx, .drf, .drw, .dtd, .dxb, .dxf, .dxg, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fmb, .fhd, .fla, .flac, .flv, .fpx, .fxg, .gray, .grey, .gry, .h, .hbk, .hpp, .ibank, .ibd, .ibz, .idx, .iif, .iiq, .incpas, .indd, .kc2, .kdbx, .kdc, .key, .kpdx, .lua, .m, .m4v, .max, .mdc, .mdf, .mef, .mfw, .mmw, .moneywell, .mos, .mov, .mp3, .mp4, .mpg, .mrw, .msg, .myd, .nd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nwb, .nx2, .nxl, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .oil, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab, .pages, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pef, .pem, .pfx, .pl, .plc, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .pptm, .prf, .ps, .psafe3, .psd, .pspimage, .ptx, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .r3d, .raf, .rat, .raw, .rdb, .rm, .rtf, .rw2, .rwl, .rwz, .s3db, .sas7bdat, .say, .sd0, .sda, .sdf, .sldm, .sldx, .sql, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .std, .sti, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxi, .sxm, .sxw, .tex, .tga, .thm, .tlg, .vob, .war, .wallet, .wav, .wb2, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlk, .xlm, .xlr, .xlsb, .xlsm, .xlt, .xltm, .xltx, .xlw, .ycbcra, .yuv
Source : Intel Security Advanced Threat Research - http://www.intelsecurity.com