Sécurité des Systèmes d'Information

Introduction & Bonnes pratiques

Dr. Cyrille CHAVET

Université Bretagne Sud

Lab-STICC

www.univ-ubs.fr

Plan du séminaire

- Concepts généraux
- Exemples d'attaques
- Bonnes pratiques
- Comment réagir en cas de problème ?

Petite introduction…

Quelques chiffres

- **Durée de vie d'un PC sous Windows ?**
  - **Avec connexion directe à internet**
  - **Sans antivirus à jour**
  - **Sans firewall**

- **En 2003 : 40 minutes**
- **En 2004 : 20 minutes**

- **En 2018 ?**

Source www.sans.org

Quelques chiffres

- Durée de vie d'un PC sous Windows ?
  - Avec connexion directe à internet
  - Sans antivirus à jour
  - Sans firewall

- En 2003 : 40 minutes
- En 2004 : 20 minutes

- En 2018 : **3 minutes**

Source www.sans.org

Quelques chiffres

➢ Coût moyen d'une « cyber-attaque » en France

- **Une attaque majeur en France tous les 15 jours**
  (Source ANSSI - https://www.ssi.gouv.fr)

→ **773 000 euros**
Enquête sur plus de 1000 entreprises dont 100 en France

NTT Communications
Transform. Transcend.

➢ Coût d'une panne majeure des SI en Europe

→ **250 milliards de dollars**

Imaginez: plus d'électricité, plus de transactions financières, plus de transports…

➢ Coût annuel du cybercrime

→ **3000 milliards de dollars en 2020**

Forum Economique Mondial

WORLD ECONOMIC FORUM

Université Bretagne Sud
ubs

Cyberdéfense / Cybersécurité

Cyberdéfense / Cybersécurité

- **Objectif**
  - **Défendre les systèmes d'informations de la nation**

Cyberdéfense / Cybersécurité

- Objectif
  - Défendre les systèmes d'informations de la nation

- Pas un concept seulement « militaire »
  - Forces armées => 10 %
  - Services spéciaux & Agences => 10 % à 20 %
  - Grands groupes, les PME/PMI…

ANSSI

- **Agence Nationale de Sécurité des Systèmes d'Information**
- **Institution de référence en France**
- **Implications**
  - **Protection de l'état et des institutions**
  - **Intervention dans les entreprises**
  - **Veilles technologiques (CERT)**
  - **Produit du contenu pour les formations informatiques, électroniques**
  - ***Participe activement à la défense de nos SI***

SecNumedu
ANSSI

SecNum académie
ANSSI

Université Bretagne Sud

Concepts généraux

Structure d'un Système d'Information

Couches sémantiques

Couches des logiciels

Couches des infrastructures

Structure d'un Système d'Information

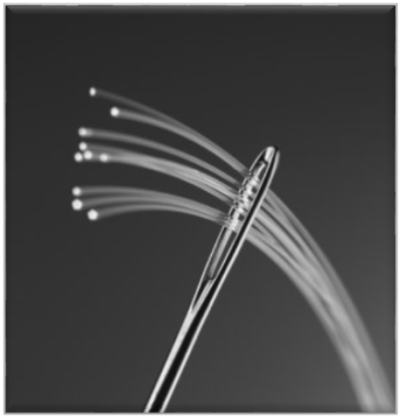
Couches sémantiques

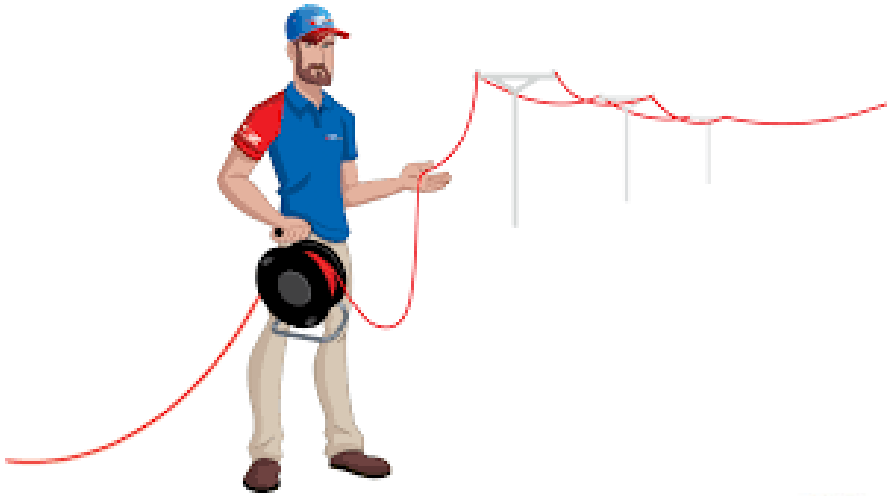
Couches des logiciels

Couches des infrastructures

Université Bretagne Sud

Couche des infrastructures





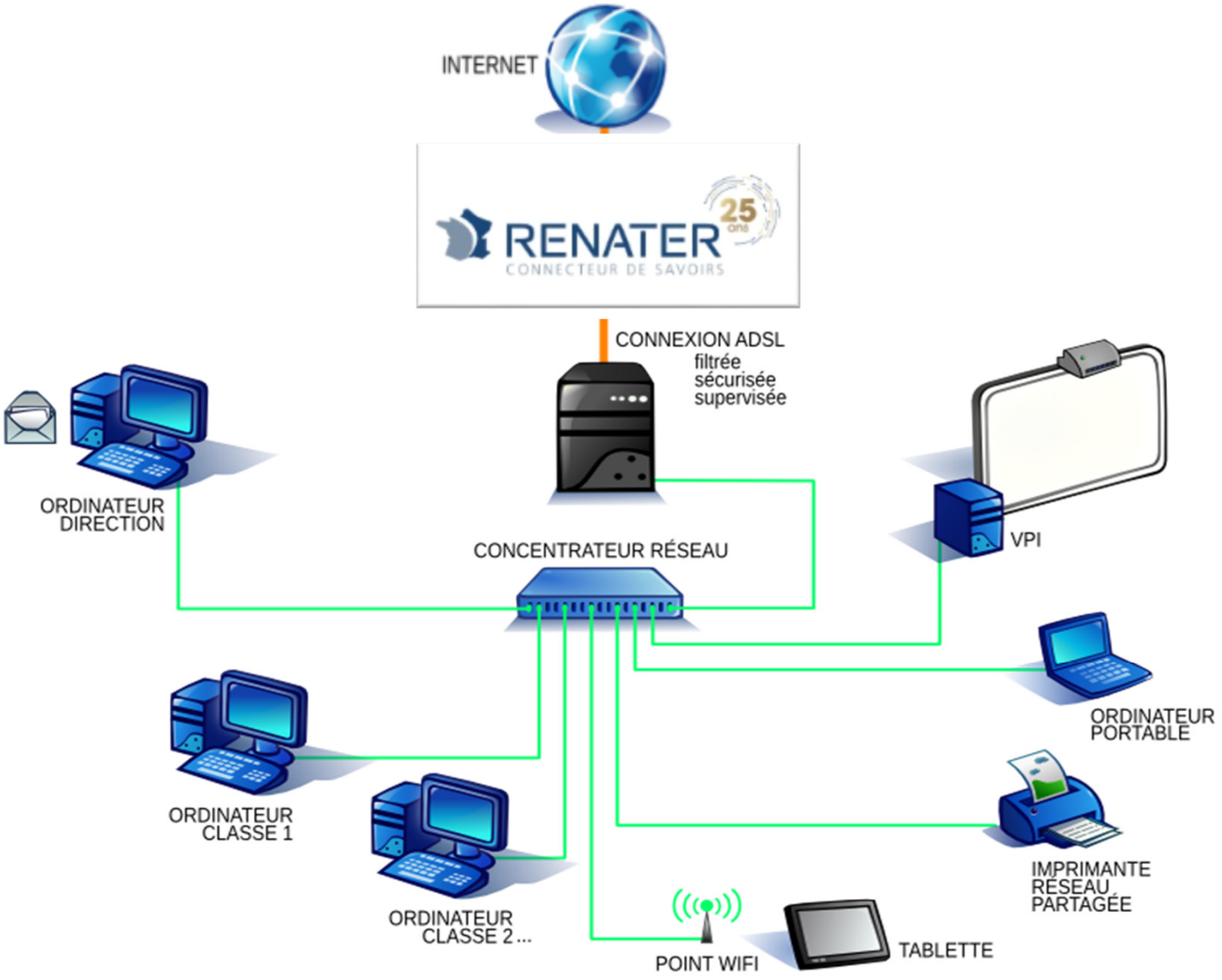
Université Bretagne Sud

RENATER

RENATER 25 ans
CONNECTEUR DE SAVOIRS

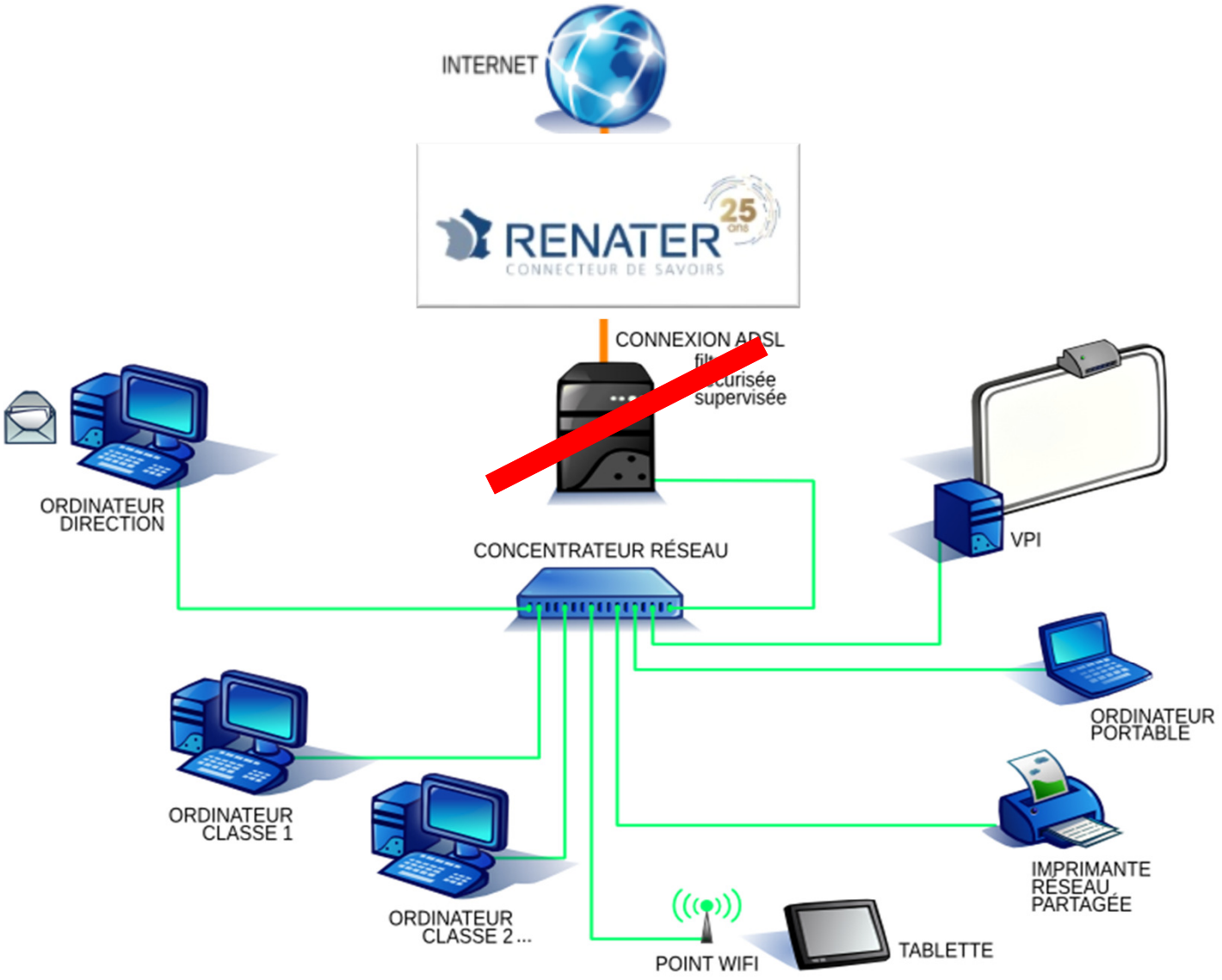
Université Bretagne Sud

Le réseau informatique UBS

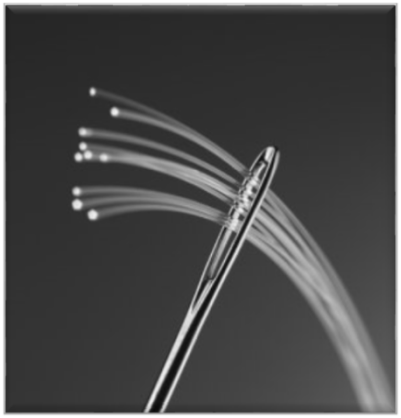


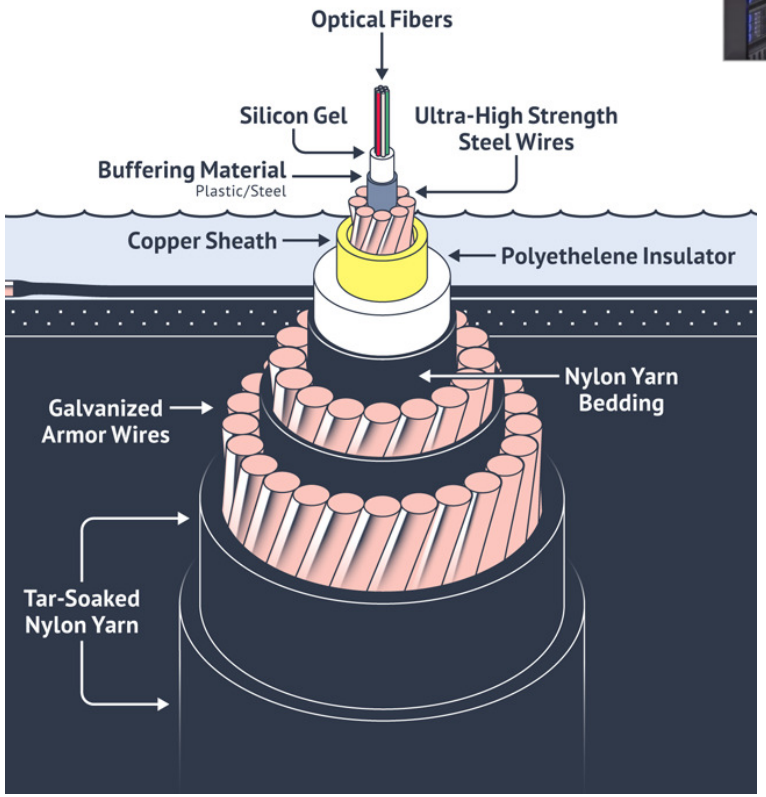
Université Bretagne Sud

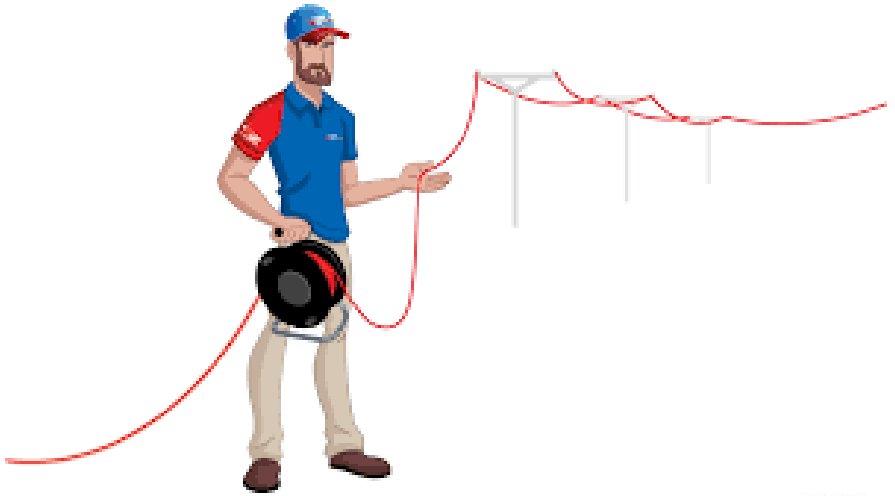
Plus d'internet à l'UBS - 2016



Couche des infrastructures

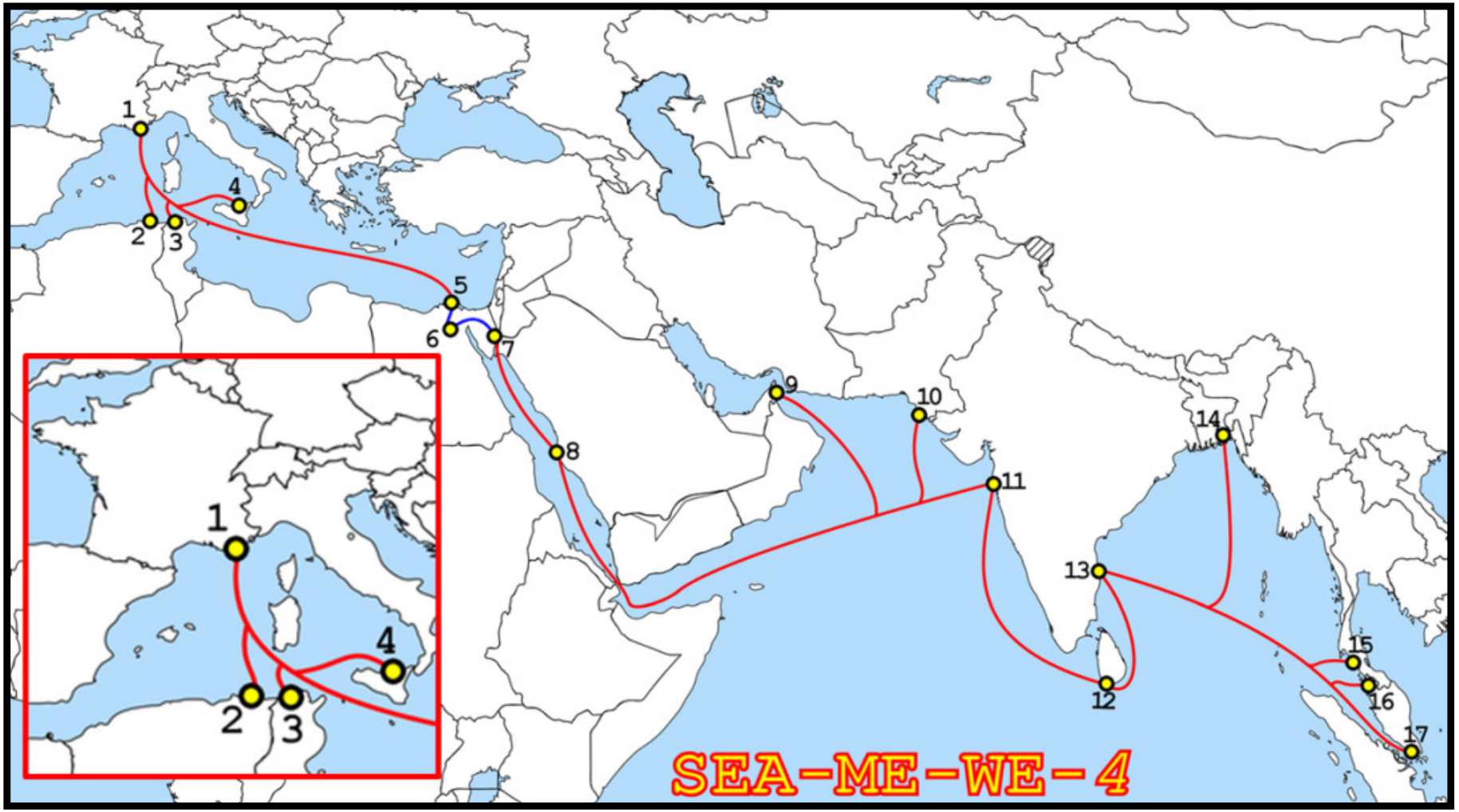






Université Bretagne Sud

Exemple de câbles « *marins* »



Source Orange

Structure d'un Système d'Information

Couches sémantiques

Couches des logiciels

Couches des infrastructures

Université Bretagne Sud

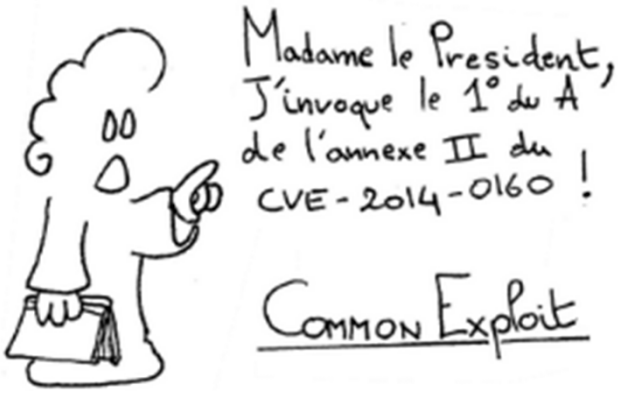
Certification Critères Communs

- **Norme ISO-15408**
- **Internationalement reconnu**
- **Objectif**
  - Evaluer la sécurité des systèmes et des logiciels informatiques
  - Assurer la sécurité d'un produit vis-à-vis d'un niveau d'assurance requis
    - Passeports biométriques, cartes bancaires…

CVE

- ***Common Vulnerabilities and Exposures***
- **Références CVE-AAAA-NNNN**
  - AAAA est l'année de publication
  - NNNN un numéro d'identifiant
- **Description succincte de la vulnérabilité**
- **Liens vers plus d'informations et recommandations**

CVE



- Base de données publique
- A disposition des éditeurs pour création de correctifs
- A disposition des chercheurs pour étudier les failles et proposer des recommandations

Université Bretagne Sud

CVE

- Base de données publique
- A disposition des éditeurs pour création de correctifs
- A disposition des chercheurs pour étudier les failles et proposer des recommandations
- A disposition des cybercriminels…

Université Bretagne Sud

Faille inconnue ou *Zero-day*

Faille inconnue ou *Zero-day*

- **Word, Powerpoint, Excel…**

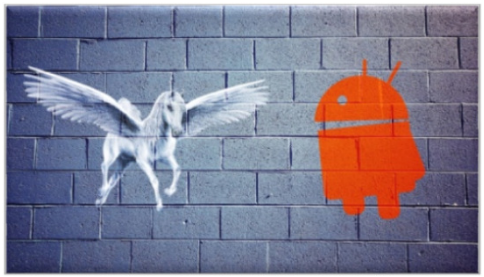
Faille inconnue ou *Zero-day*

- Word, Powerpoint, Excel…
- Facebook
- What'sApp

Université Bretagne Sud

Faille inconnue ou *Zero-day*

- Word, Powerpoint, Excel…
- Facebook
- What'sApp
- Pegasus



Université Bretagne Sud

Structure d'un Système d'Information

Couches sémantiques

Couches des logiciels

Couches des infrastructures

Université Bretagne Sud

Fake news

- **Piratage du compte Twitter de *Associated press* en 2012**

- **High frequency trading *(cf. vidéo Eureka: « Trading à la vitesse de la lumière »)***

Problèmes de sureté/sécurité

Couches sémantiques

Couches des logiciels

Couches des infrastructures

Université Bretagne Sud

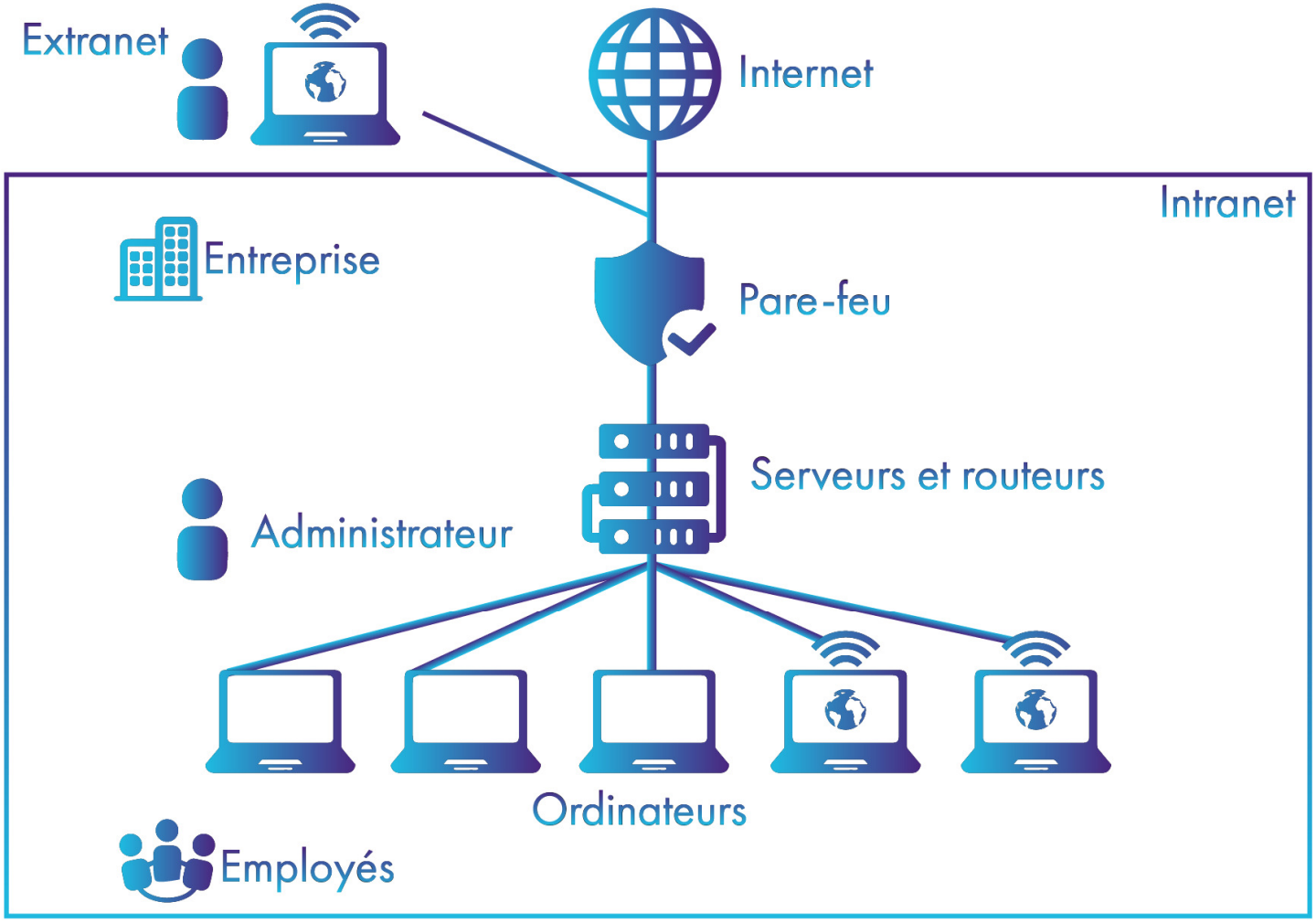
Un peu de vocabulaire

Réseau informatique

Kézako ?

Université Bretagne Sud

Réseau informatique



Notions de cyber-sécurité (1)

- **Sureté ≠ Sécurité**

- **Sureté** (***Système immunitaire***)
  - Le système est conçu pour pouvoir fonctionner malgré des ***pannes naturelles***

- **Sécurité** (***Vaccins***)
  - Le système est conçu pour pouvoir résister aux ***attaques volontaires*** d'individus malintentionnés

Notions de cyber-sécurité (2)

- **Virus ≠ Vers**
- **Virus**
  - Logiciel pouvant causer des (gros) dégâts s'il est exécuté
  - Mais il est incapable de se propager seul

Notions de cyber-sécurité (2)

- **Virus ≠ Vers**
- **Virus**
  - Logiciel pouvant causer des (gros) dégâts s'il est exécuté
  - Mais il est incapable de se propager seul
- **Vers (Worms)**
  - Logiciel pouvant causer des (gros) dégâts s'il est exécuté
  - Il sait se répliquer, se cacher, se métamorphoser et se répandre seul de machine en machine…

Notions de cyber-sécurité (3)

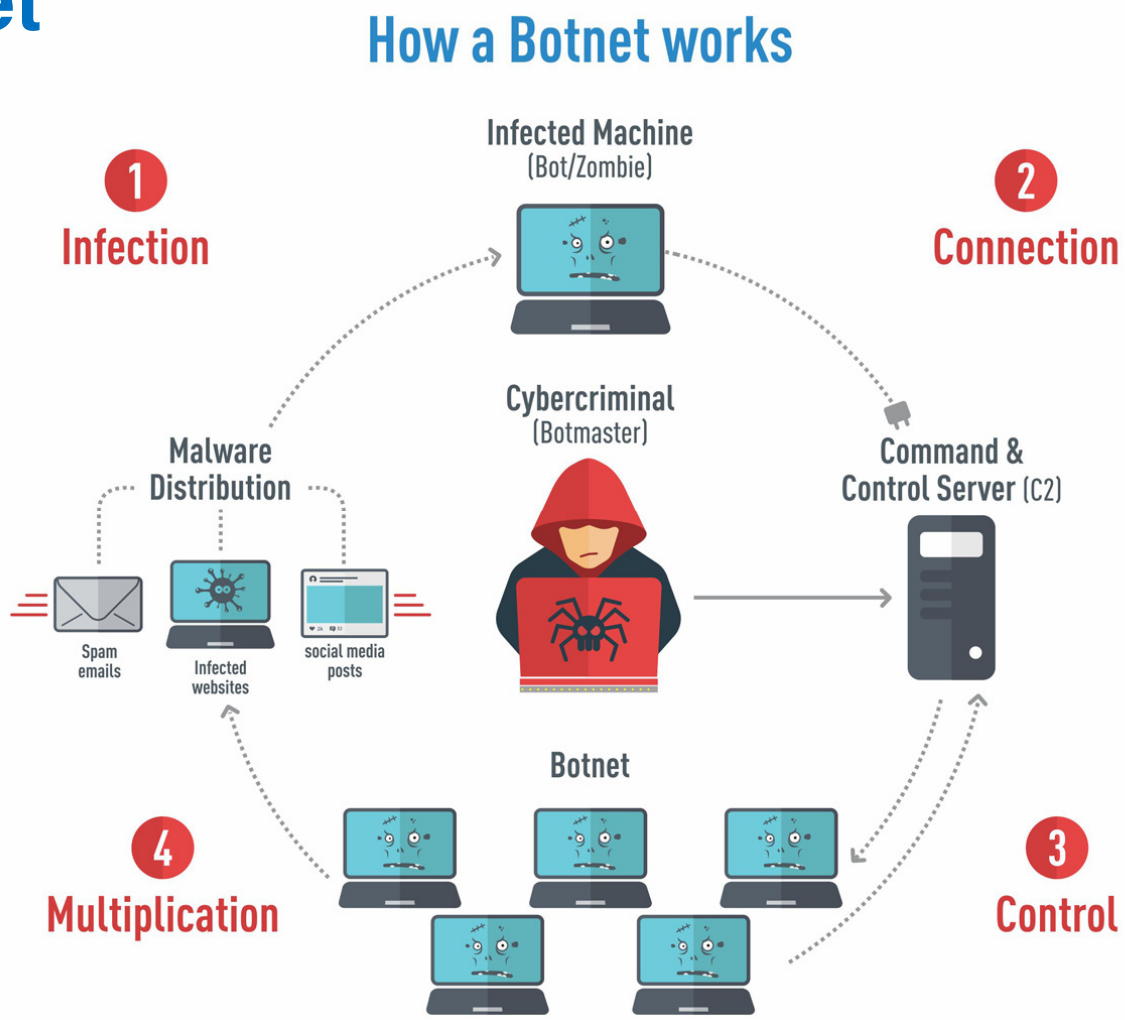
- **Chevaux de Troie (Trojan)**
  - Virus ou vers

- **Ouverture de « portes » pour des attaques**

Université Bretagne Sud

Notions de cyber-sécurité (3)

➢ Botnet



Source: EMISOFT

Notions de cryptologie

Notions de cryptologie

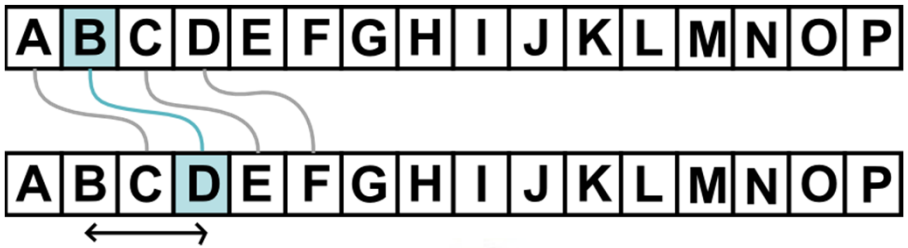
- **Cryptographie**
  - Chiffrement/déchiffrement d'un message
- **Cryptanalyse**
  - Décryptage ou *hackage* d'un message chiffré
- **La cryptologie permet**
  - De protéger des informations en les rendant illisibles
  - De garantir la sécurité des systèmes d'information et le secret des sources
  - D'assurer la confidentialité, l'authentification de l'auteur du message et son intégrité

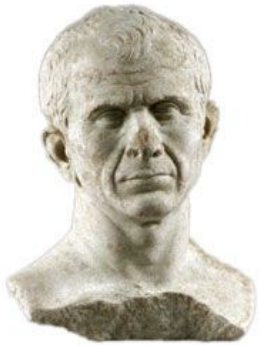
Les premiers pas

- **Chiffrement par offuscations/substitutions**

Les premiers pas

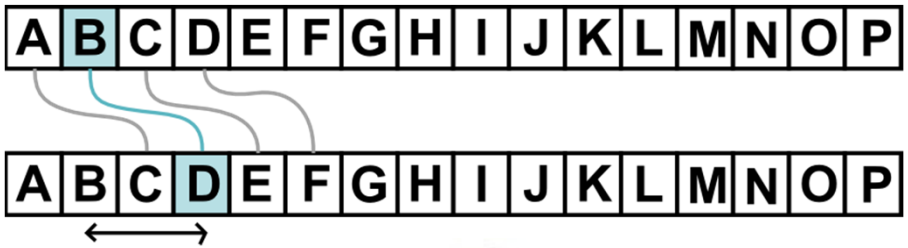
- **Chiffrement par offuscations/substitutions**

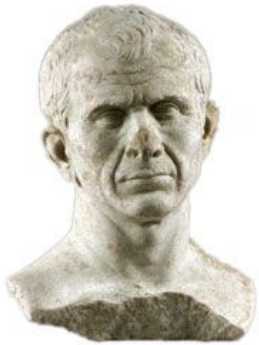




Les premiers pas

- **Chiffrement par offuscations/substitutions**



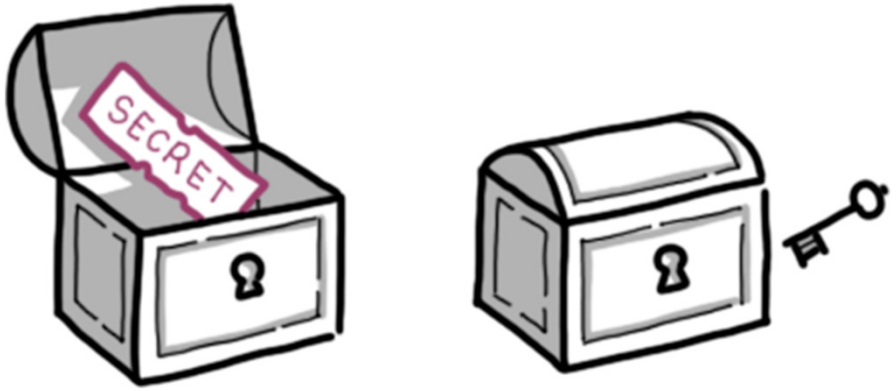


Université Bretagne Sud

La cryptographie moderne

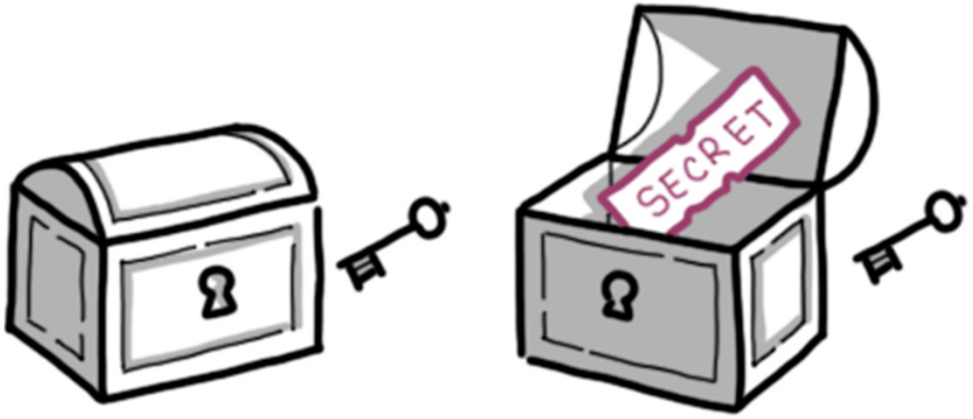
- **Principe de Kerckhoffs :**
  - « *La sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef.* »

- **Tous les autres paramètres doivent être supposés publiquement connus**



Notions de *clef*

- Tout algorithme de chiffrement (resp. déchiffrement) utilise un ensemble de *clefs* ou *mots de passe*
- On parle de *clefs de chiffrement (resp. déchiffrement)*



Université Bretagne Sud

Notions de cryptographie (1)

- **Symétrique**
  - La même clé est utilisée pour chiffrer et déchiffrer le message

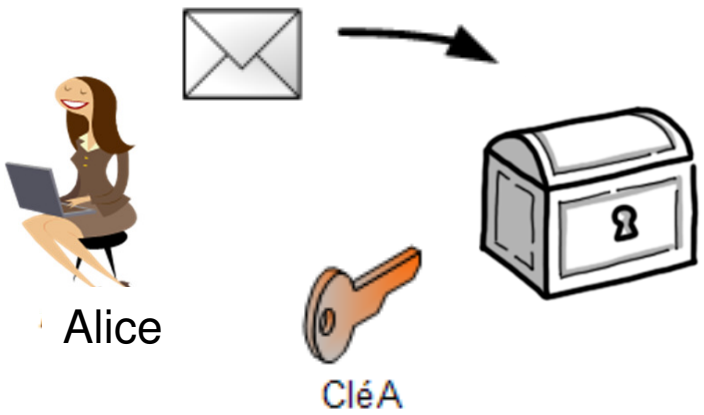
Alice

Bob

Université Bretagne Sud

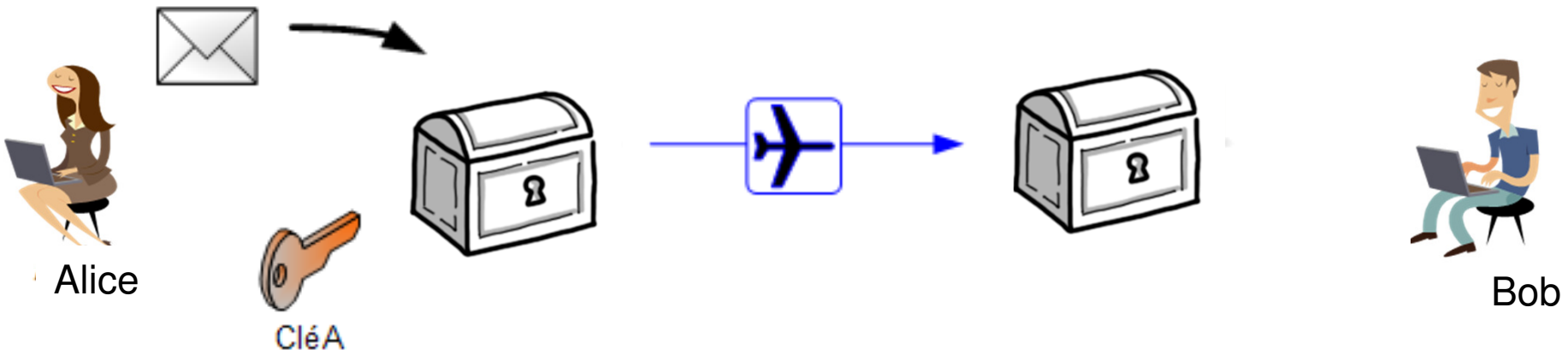
Notions de cryptographie (1)

- **Symétrique**
  - La même clé est utilisée pour chiffrer et déchiffrer le message



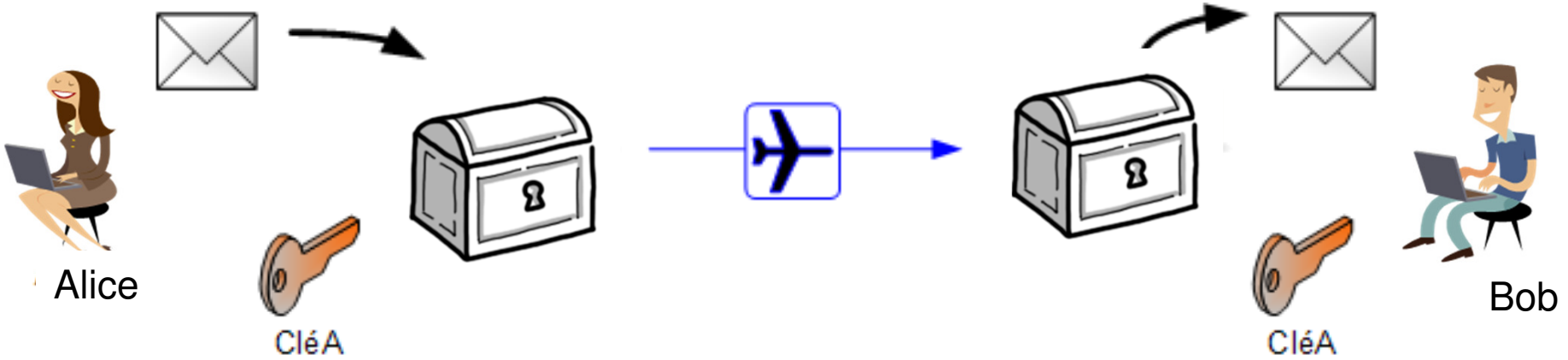
Notions de cryptographie (1)

- **Symétrique**
  - La même clé est utilisée pour chiffrer et déchiffrer le message



Notions de cryptographie (1)

- **Symétrique**
  - La même clé est utilisée pour chiffrer et déchiffrer le message



Notions de cryptographie (2)

- **Idée de la cryptographie symétrique**
  - La même clé est utilisée pour fermer et ouvrir le « coffre » contenant le message à protéger
  - **La clef doit rester secrète**

- **Algorithmes**
  - **AES**, DES…

Notions de cryptographie (3)

- **Asymétrique**
  - Une **clef publique** et une **clef privée** (ou **secrète**)

Notions de cryptographie (3)

- **Asymétrique**
  - Une **clef publique** et une **clef privée** (ou **secrète**)

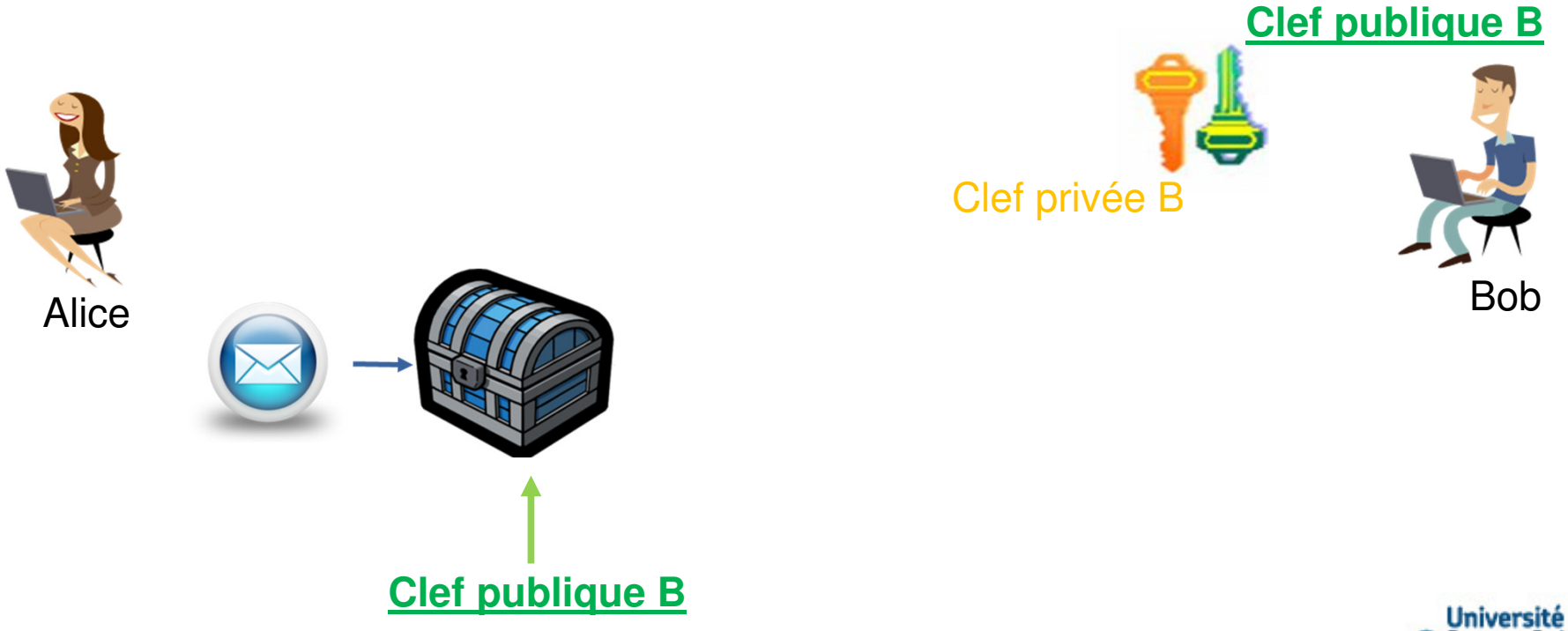
Notions de cryptographie (4)

➢ Idée de la cryptographie asymétrique

- Une **clef publique** (fermeture) et une **clef privée** (ouverture)

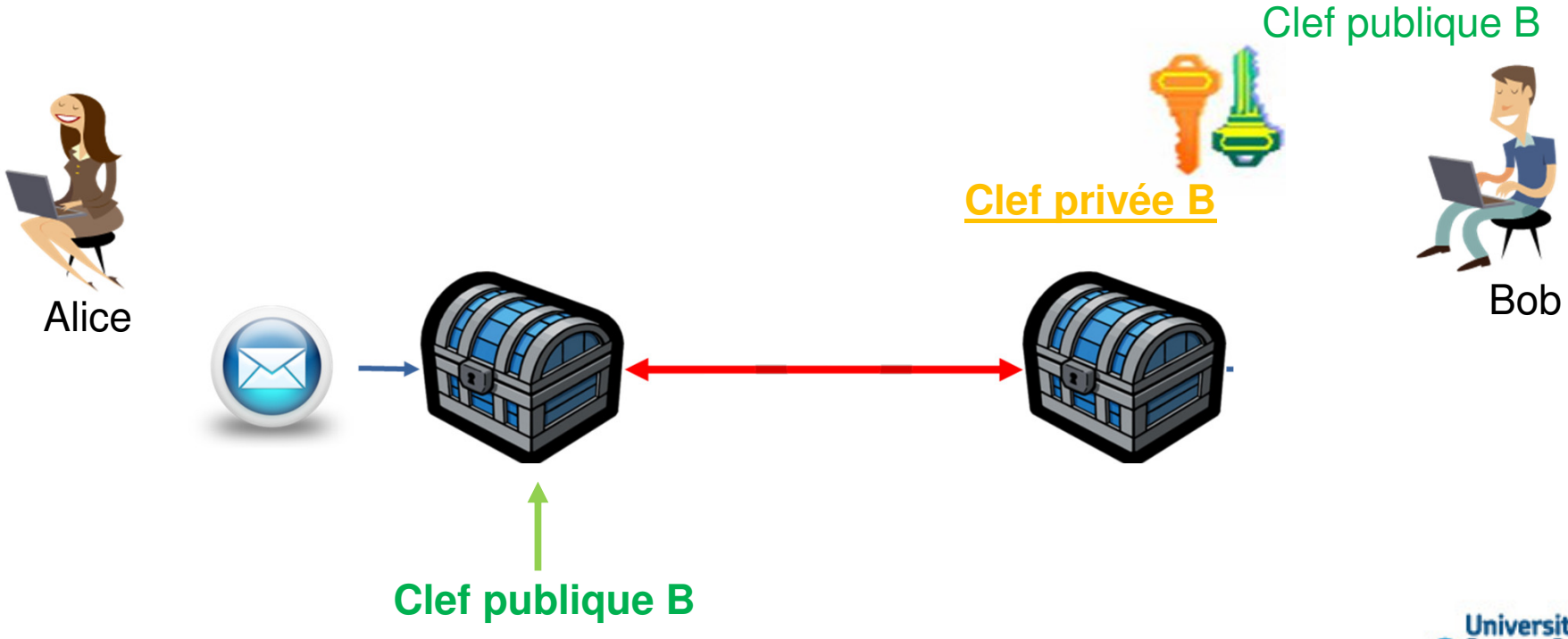
Notions de cryptographie (4)

- **Idée de la cryptographie asymétrique**
  - Une **clef publique** (fermeture) et une **clef privée** (ouverture)



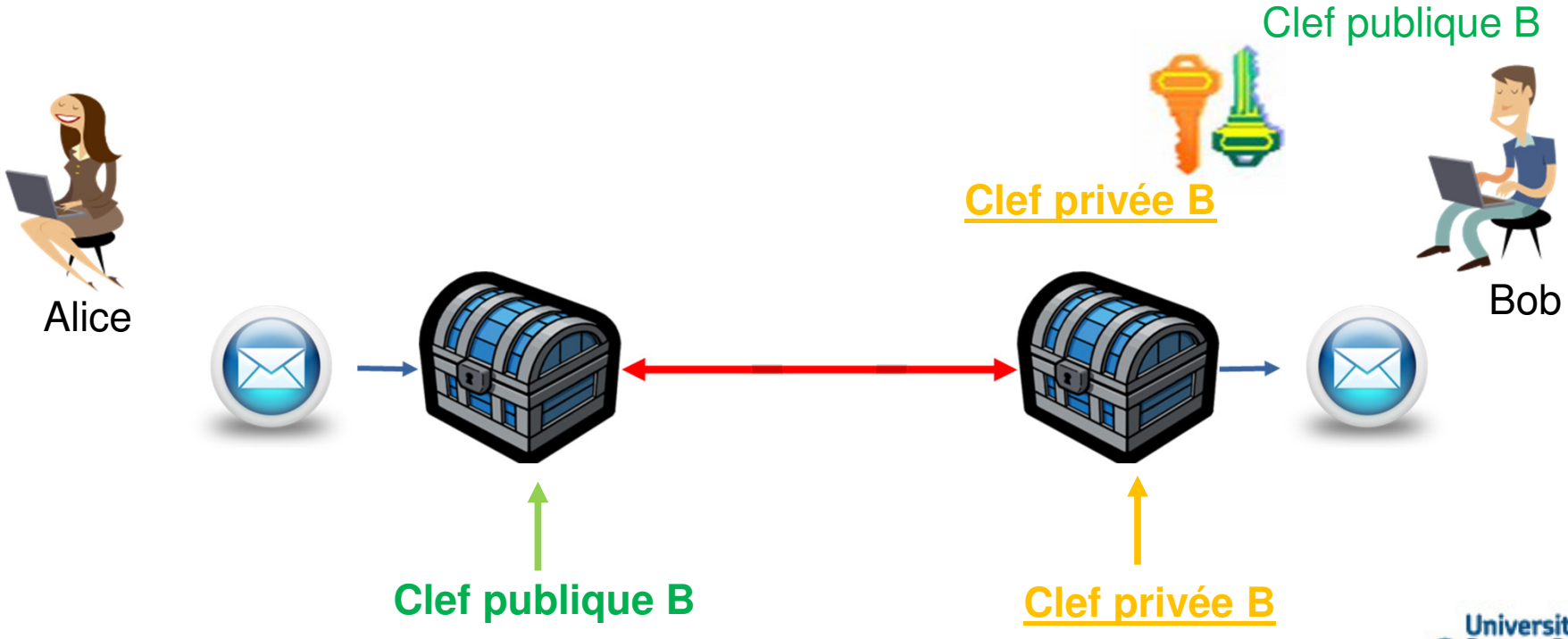
Notions de cryptographie (4)

- **Idée de la cryptographie asymétrique**
  - Une **clef publique** (fermeture) et une **clef privée** (ouverture)



Notions de cryptographie (4)

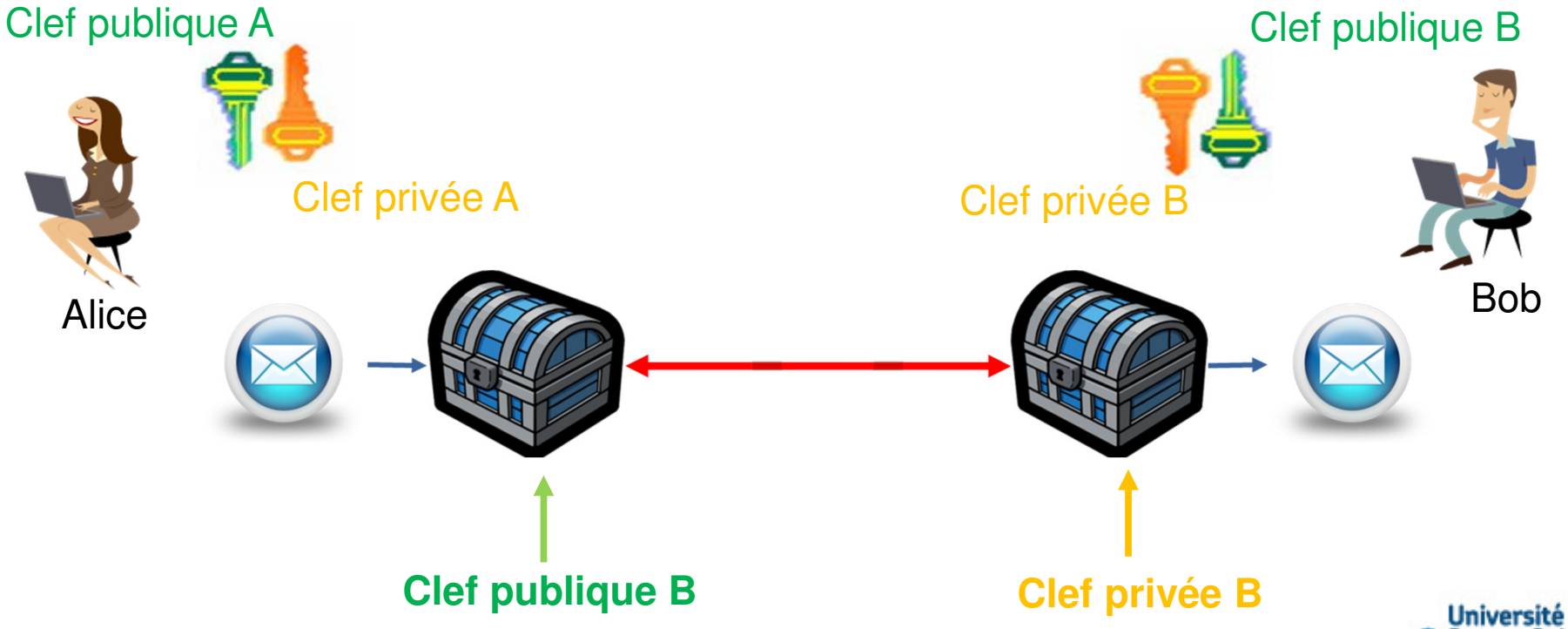
- **Idée de la cryptographie asymétrique**
  - Une **clef publique** (fermeture) et une **clef privée** (ouverture)



Notions de cryptographie (4)

➢ Idée de la cryptographie asymétrique

- Une **clef publique** (fermeture) et une **clef privée** (ouverture)



Notions de cryptographie (5)

- **Idée de la cryptographie asymétrique**
  - Une **clef publique** (fermeture) et une **clef privée** (ouverture)

- **Algorithmes**
  - **RSA**, PGP, OpenSSL…

Sécurité « mathématiques »

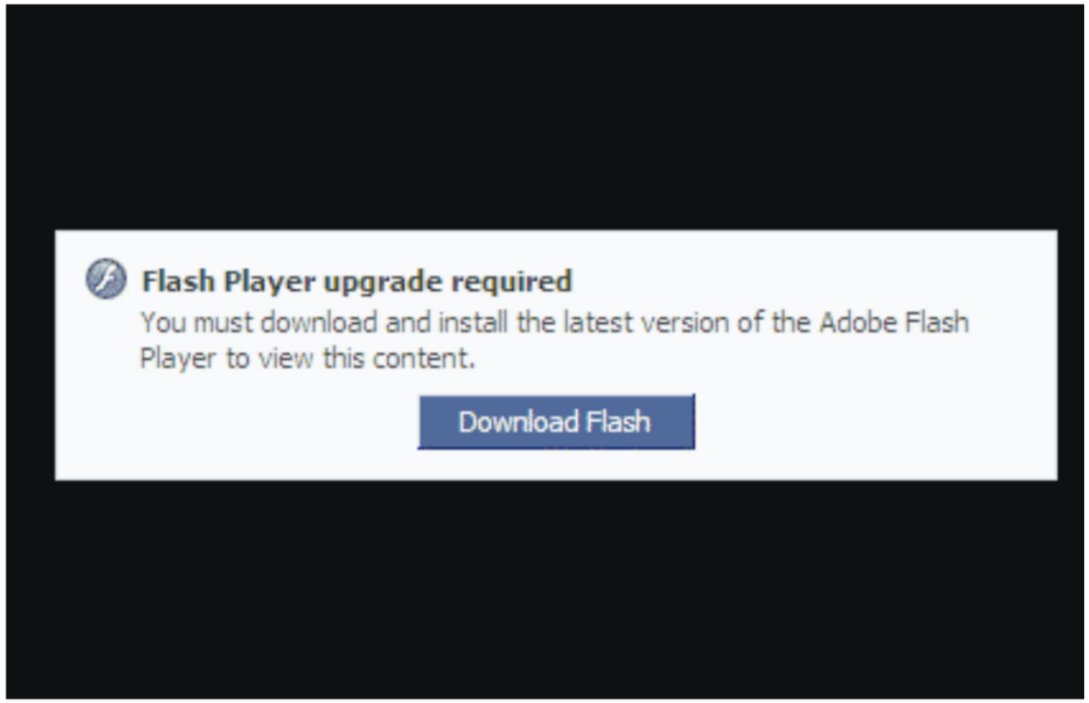
- **Basées sur des problèmes mathématiques connus pour être très complexes***
  - Calcul de décomposition de produits de facteurs premiers très grand
  - Calcul de logarithmes discrets sur des corps finis
  - Calcul de points sur courbes elliptiques
  - Calcul homomorphe
  - Recherche de plus court vecteur dans un espace euclidien
  - …

*** Pour des machines classiques…**

Une attaque c’est quoi ?

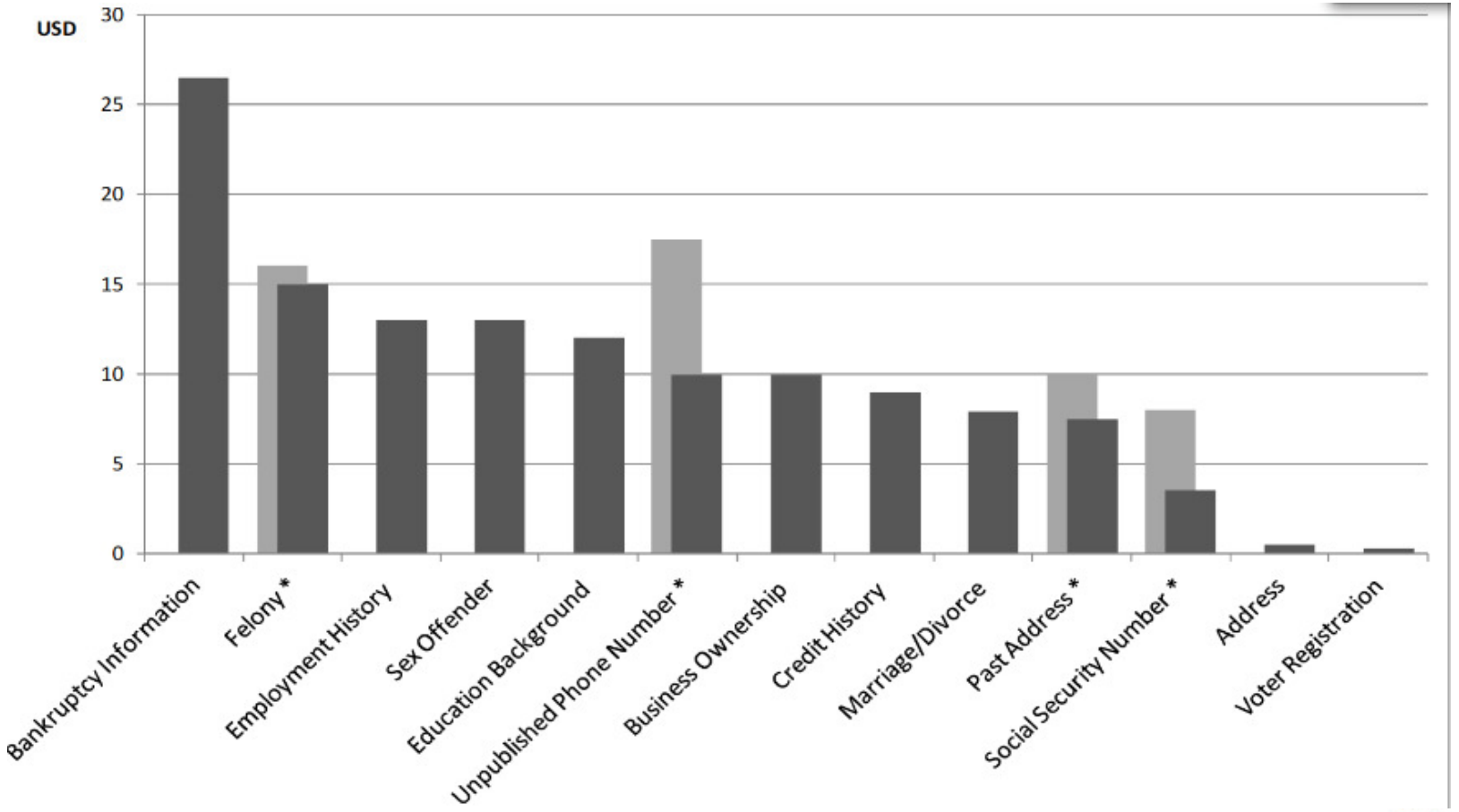
Une bonne attaque

- **Ingénierie sociale**



Une bonne attaque

➢ Ingénierie sociale



Université Bretagne Sud

Une bonne attaque

- **Ingénierie sociale**

5 milliards $ CA,
90 pays, 95% des ménages

Une bonne attaque

- **Ingénierie sociale**

5 milliards $ CA,
90 pays, 95% des ménages

1,2 milliards $ CA,
700 millions de personnes,
3000 éléments sur chaque consommateur US

Université Bretagne Sud

Une bonne attaque

➢ Ingénierie sociale

5 milliards $ CA,
90 pays, 95% des ménages

1,2 milliards $ CA,
700 millions de personnes,
3000 éléments sur chaque consommateur US

…

Université Bretagne Sud
ubs

Protection de la vie privée

➢ Directives européennes

Une bonne attaque (2)

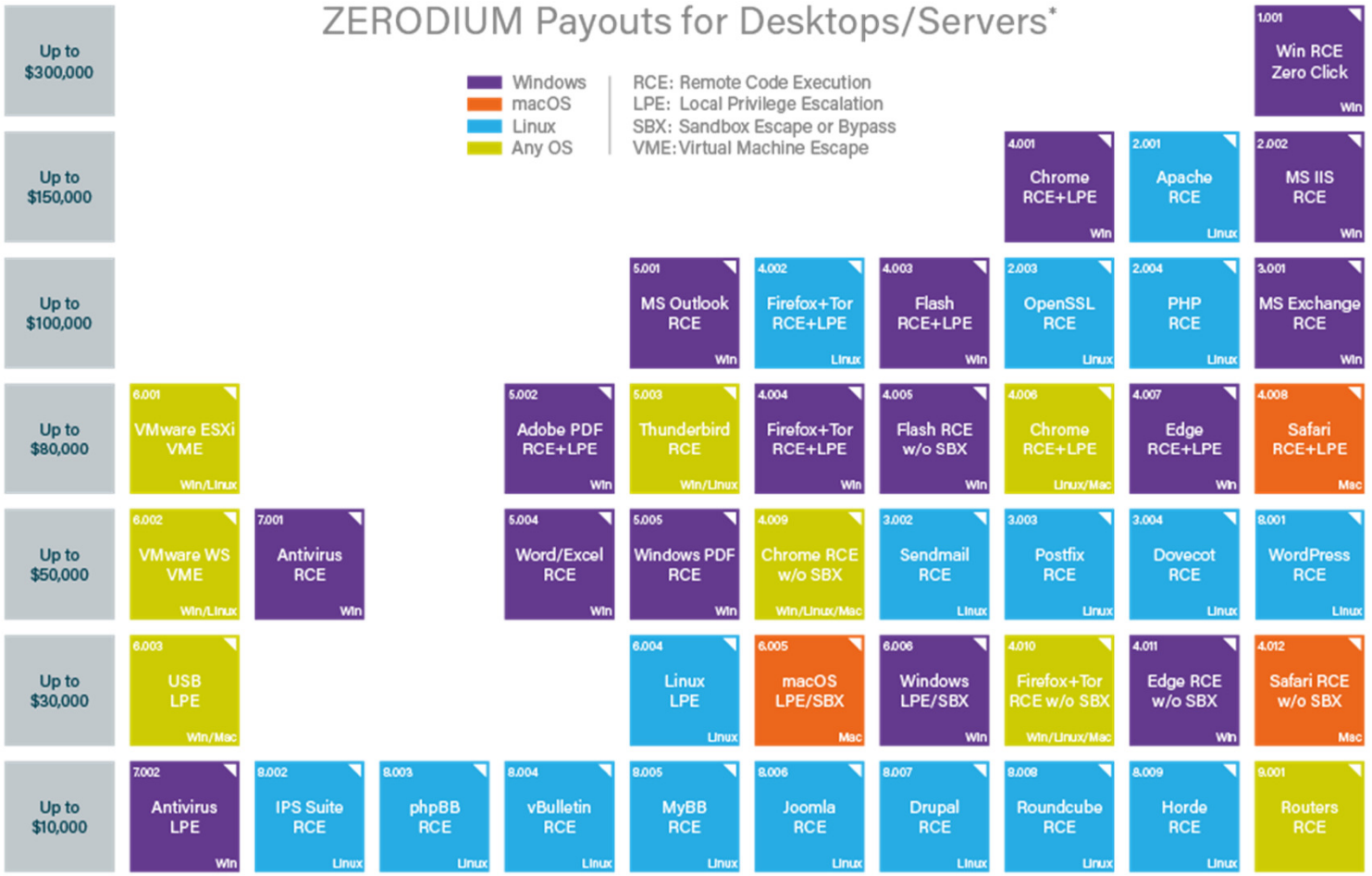
- **Ingénierie sociale**
- **Connaitre des failles dans le système**
  - CVE
  - Trouver des failles *0-day*

Bug bounty

- Prime aux découvreurs de bug inconnus

Bug bounty

➢ Prime aux découvreurs de bug inconnus



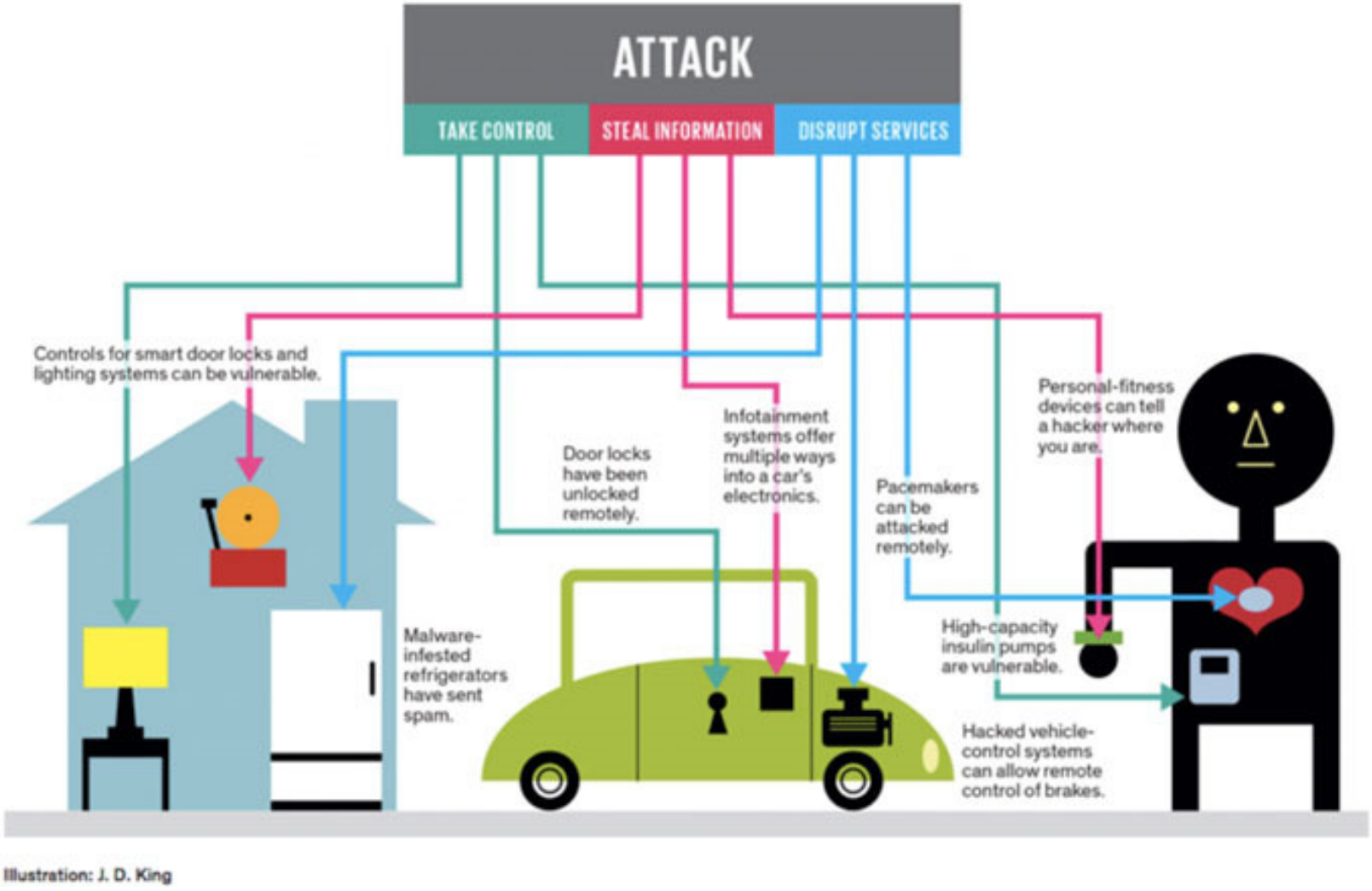
Failles zero-day: 10K€ à 1,5M€

Université Bretagne Sud

Attaquer pourquoi faire ?

- Extorsion de fonds
- Espionnage (industriel ou entre état)
- Obstruction/Destruction

Notion de surface d'attaque



Source: Alan GRAU – IEEE Spectrum

Notion de type d'attaque

- **Exploit d'un CVE**

Notion de type d'attaque

- **Exploit d'un CVE**

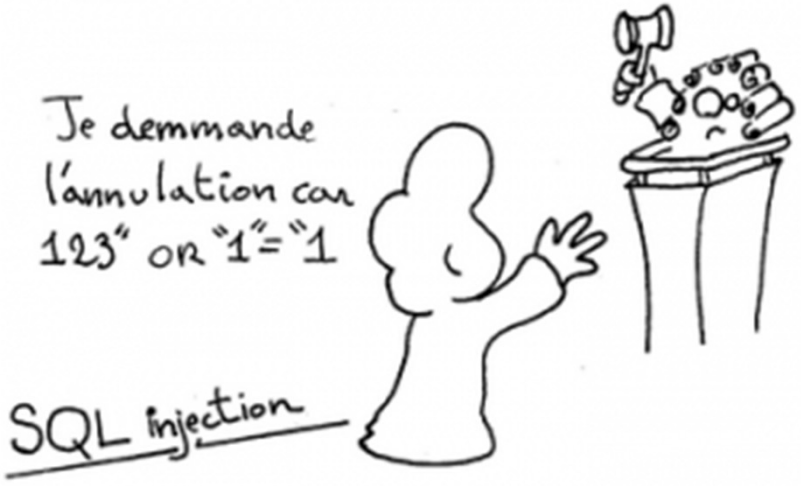
- **Dénis de service (DDOS)**

Notion de type d'attaque

- **Exploit d'un CVE**

- **Dénis de service (DDOS)**

- **Exploit par injection**

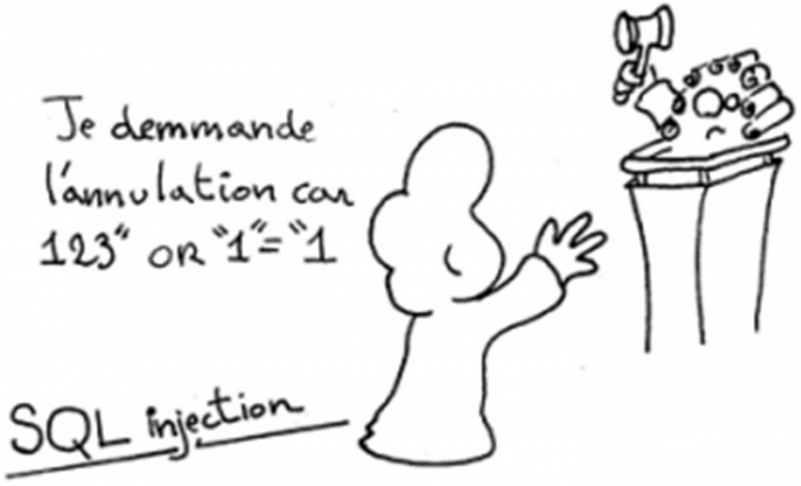


Notion de type d'attaque

- **Exploit d'un CVE**

- **Dénis de service (DDOS)**

- **Exploit par injection**

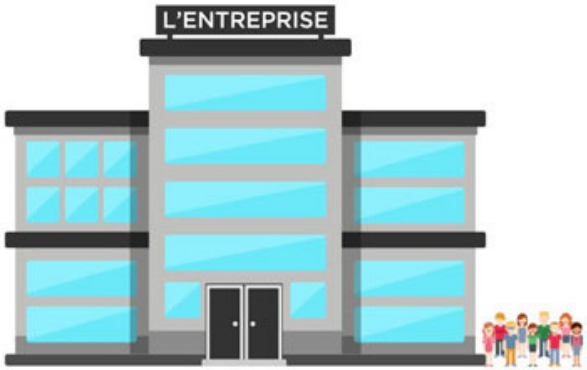


- **Exploit *zero-day*…**

Exemples d’attaques

Le botnet bancaire Dridex

Dridex



Transfert 1,4 M€

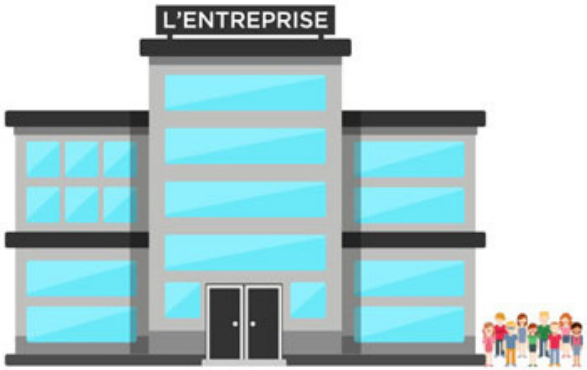
Suisse

Allemagne

Europe de l'est

cf. www.sekoia.fr

Dridex



Transfert 1,4 M€

2FA

Suisse

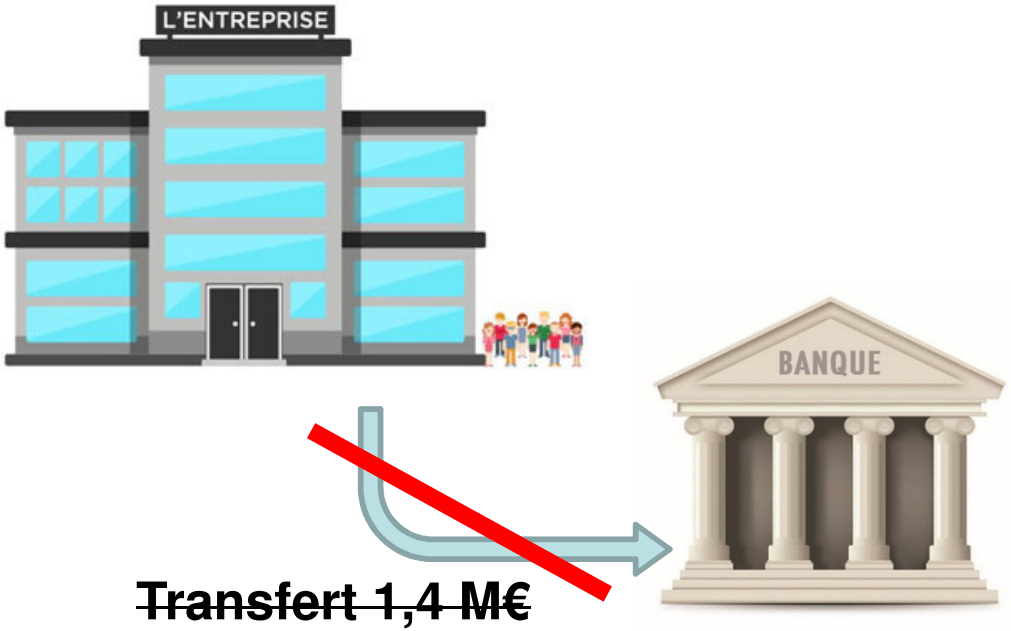
Allemagne

Europe de l'est

cf. www.sekoia.fr

Université Bretagne Sud

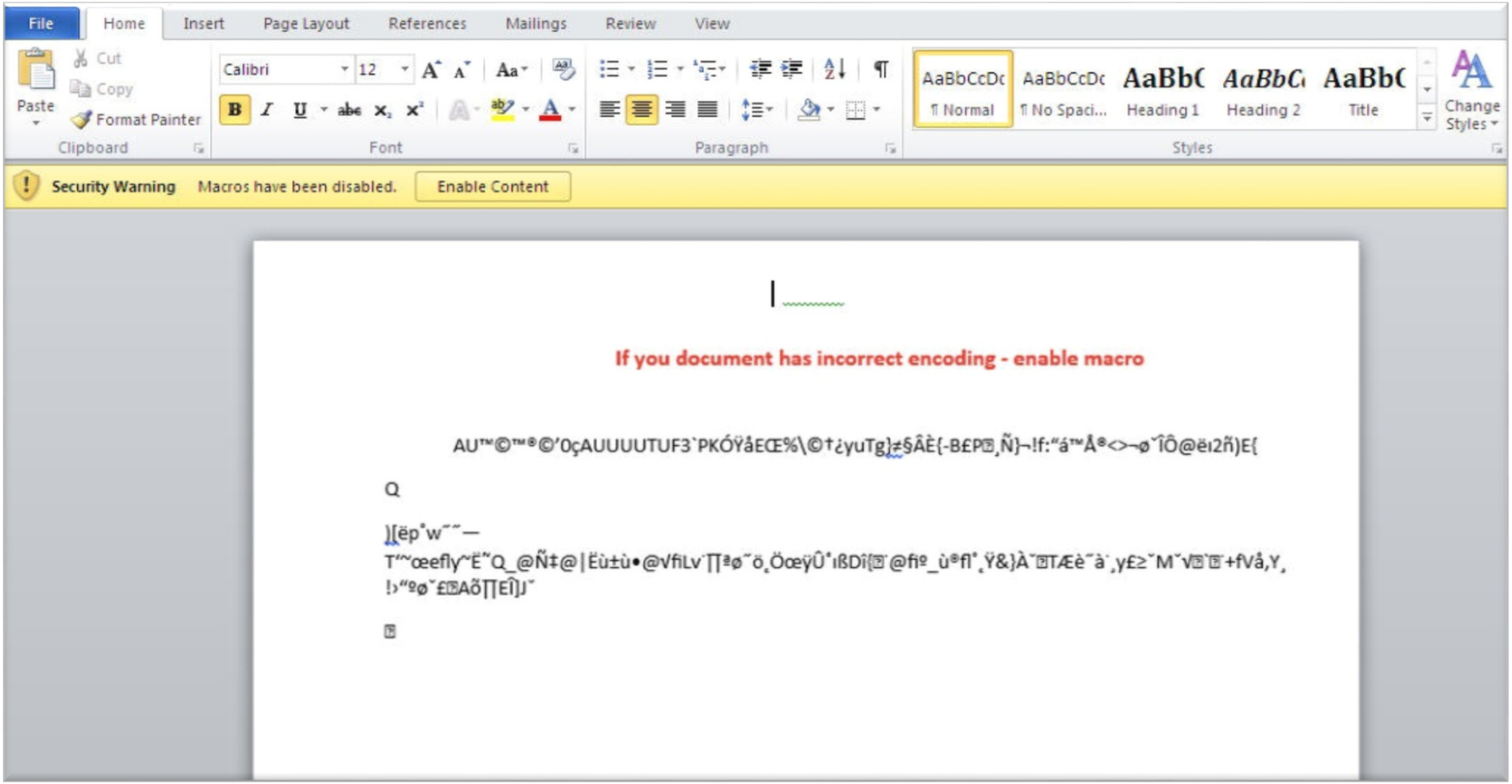
Dridex



Comment est-ce possible ?

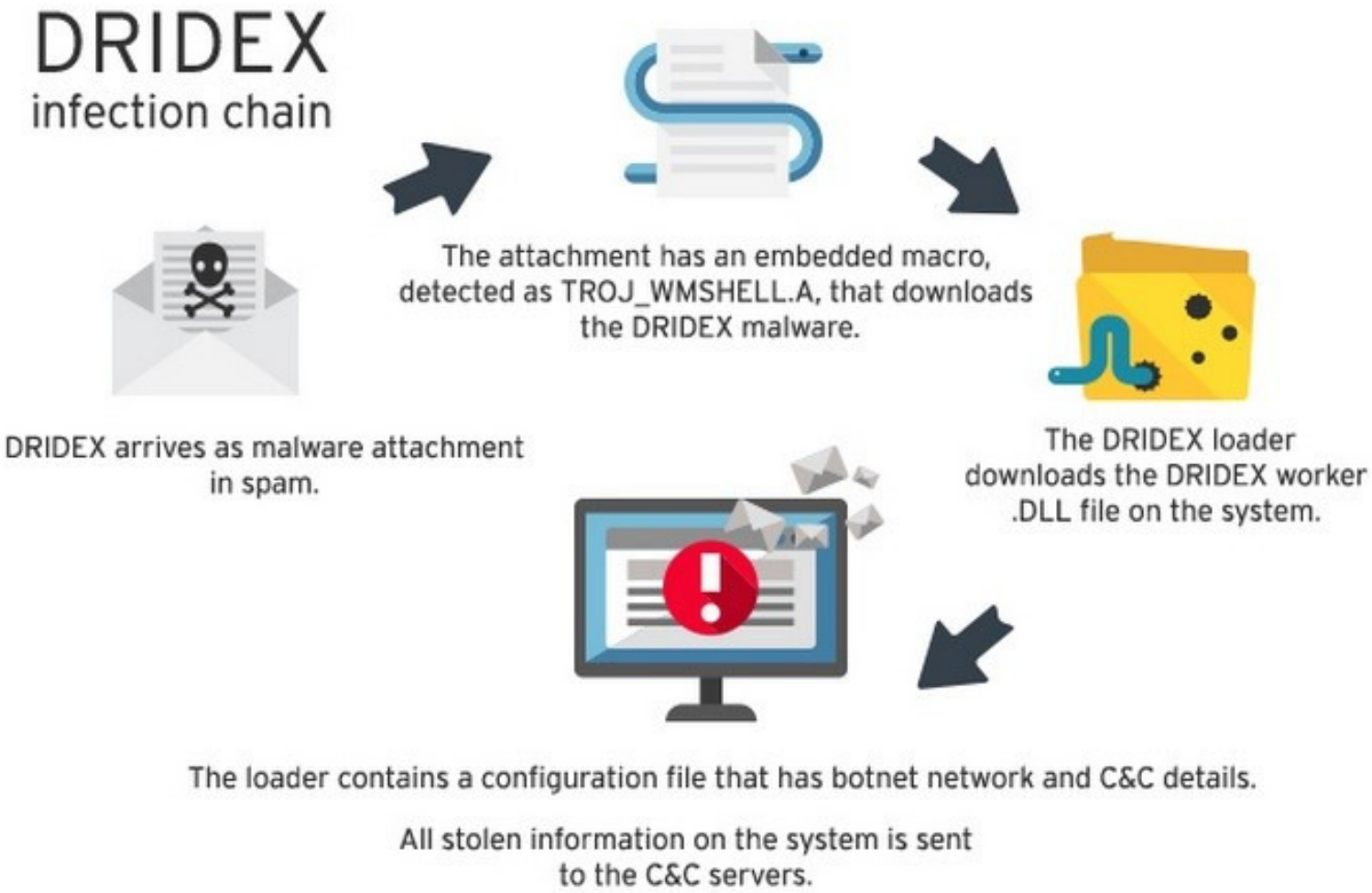
Source: https://securityaffairs.co

Comment est-ce possible ?



Source: http://www.threattracksecurity.com

Comment est-ce possible ?



Source: https://www.cyber.nj.gov

Bilan Dridex

- Dridex cible plutôt les réseaux bancaires
- Botnet qui spam dans tous les sens

Bilan Dridex

- Dridex cible plutôt les réseaux bancaires
- Botnet qui spam dans tous les sens
- Ingénierie sociale pour faire ouvrir le fichier

Bilan Dridex

- Dridex cible plutôt les réseaux bancaires
- Botnet qui spam dans tous les sens
- Ingénierie sociale pour faire ouvrir le fichier
- Prise en main du PC par Dridex

Université Bretagne Sud

Bilan Dridex

- Dridex cible plutôt les réseaux bancaires
- Botnet qui spam dans tous les sens
- Ingénierie sociale pour faire ouvrir le fichier
- Prise en main du PC par Dridex

Phishing

- **Spamming d'e-mails pour vous tenter**
- **Vous cliquez sur le lien, vous ouvrez le pdf, vous activez une macro…**

Phishing

- **Spamming d'e-mails pour vous tenter**
- **Vous cliquez sur le lien, vous ouvrez le pdf, vous activez une macro…**
- **… et vous êtes mort.**

Déjà vu précédemment ?
Pourtant cela fonctionne toujours!

Quelques *attaques*


RANSOMWARE

WannaCry (2017)

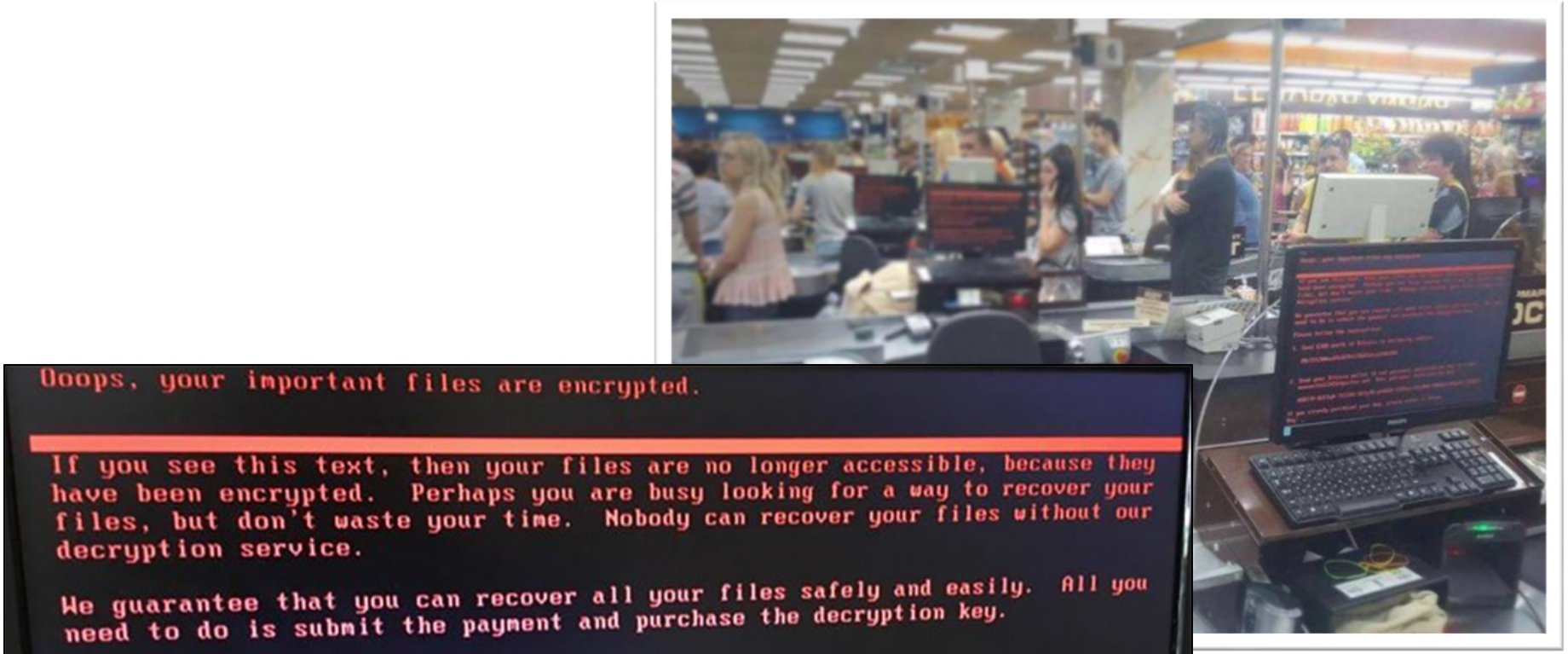
WannaCry (2017)

- **Quelques victimes**
  - **Hôpitaux britanniques**
  - **FedEx**
  - **Le système bancaire et le ministère de l'intérieur russe**
  - **Universités chinoises**
  - ***Telefonica***
  - ***Deutsche Bahn***
  - ***Renault***

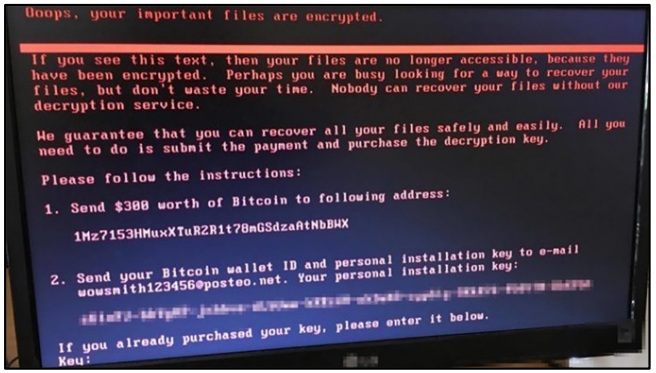
WannaCry (2017)

- **Principe**
  - Utilise des *0-day* de Windows
  - Exploite des outils de piratage volés à la NSA
- **Solution**
  - Trouvée en analysant le code du virus
  - WannaCry disposait d'un *Killswitch*
- **Qui ?**
  - La Corée du nord ?

NotPetya (2017)

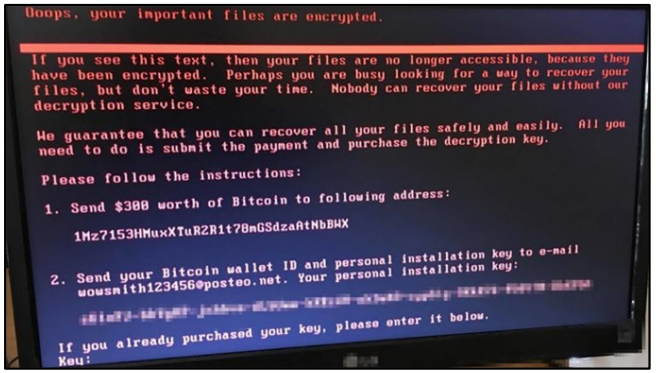


NotPetya (2017)



- RansomWare ?

NotPetya (2017)



- **RansomWare ?**
  - **NON, un « wiper »**
- **Objectif réel ?**
  - **Destruction des fichiers et des disques durs**
- **Qui ?**
  - **Un groupe de pirates *en liens avec la Russie…***
- **Comment ?**
  - **Utilise des 0-day de Windows**
  - **Exploite des outils de piratage volés à la NSA**

Université Bretagne Sud

Attaque Russe sur *l'Ukraine*

- **Principe**
  - Cible des logiciels de gestion comptable

- **Conséquences**
  - Le système bancaire est HS
  - Les aéroports doivent au mieux fortement réduire leurs activités
  - La quasi-totalité des entreprises du pays sont touchées…
    … ainsi que les filiales de groupes étrangers

Université Bretagne Sud

Conséquences sur *St Gobain*

➢ Impact

- **Système de gestion et de production à l'arrêt pendant quelques jours**
- **Pertes : 220 millions** d'euros de chiffre d'affaires et **80 millions** d'euros de résultat

➢ Mise en place d'un plan de cyberdéfense

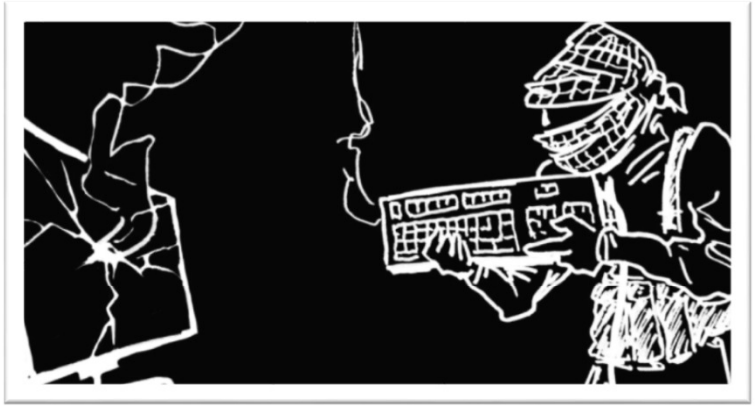
« Nous avons été touchés, nous avons chutés et nous nous sommes relevés » *(dixit N. Fernandez, directeur Cybersécurité chez St Gobain)*

Nouvelle forme de guerre

- **Ukraine sous pression permanente**
  - Cyber-Attaques de centrales électriques
  - Cyber-Attaques des systèmes bancaires
  - Cyber-Attaques de systèmes industriels
  - …
- **En plus des implications de militaires russes**
  - Annexion de la Crimée
  - État de guerre permanente dans la région du Donbass

Attaque sur *TV5 Monde (2015)*

Attaque sur *TV5 Monde (2015)*



Université Bretagne Sud

Attaque sur *TV5 Monde (2015)*

- **Attaques**
  - **Phishing**
  - **Un/plusieurs journalistes activent sans le savoir un vers**
  - **Propagation dans le réseau informatique…**

Attaque sur *TV5 Monde (2015)*

- **Attaques**
  - Phishing
  - Un/plusieurs journalistes activent sans le savoir un vers
  - Propagation dans le réseau informatique…
  - … et trouve que le réseau utilisé par les journalistes et lié aux serveurs qui gère la partie « industrielle »

Attaque sur *TV5 Monde (2015)*

- **Attaques**
  - Phishing
  - Un/plusieurs journalistes activent sans le savoir un vers
  - Propagation dans le réseau informatique…
  - … et trouve que le réseau utilisé par les journalistes et lié aux serveurs qui gère la partie « industrielle »

- **Intervention en urgence**
  - ANSSI
  - Airbus Defense and Space

Attaque sur *TV5 Monde (2015)*

- **Plus d'internet à TV5 monde pendant presque 4 mois**

- **Coût**
  - **Presque plus de revenus publicitaires**
  - **Nouvelles architectures de réseaux sécurisés**
  - **Cyber-assurances**
    - **4,6 millions d'euros en 2015**
    - **3,1 millions d'euros en 2016**
    - **2,5 millions d'euros/an à partir de 2017**

Attaque sur *TV5 Monde (2015)*

- **Plus d'internet à TV5 monde pendant presque 4 mois**
- **Coût**
  - **Presque plus de revenus publicitaires**
  - **Nouvelles architectures de réseaux sécurisés**
  - **Cyber-assurances**
    - **4,6 millions d'euros en 2015**
    - **3,1 millions d'euros en 2016**
    - **2,5 millions d'euros/an à partir de 2017**
- **Un petit clique dans un fichier, une grosse claque !**

Attaque sur *TV5 Monde (2015)*

- **Après enquête**
  - Attaques d'un groupe de pirates russes
  - Un groupe nommé APT28 (Fancy bear ou Pawn Storm …)
- **Motivation**
  - Lié à la rupture du contrat de vente de navires de guerre entre la France et la Russie…

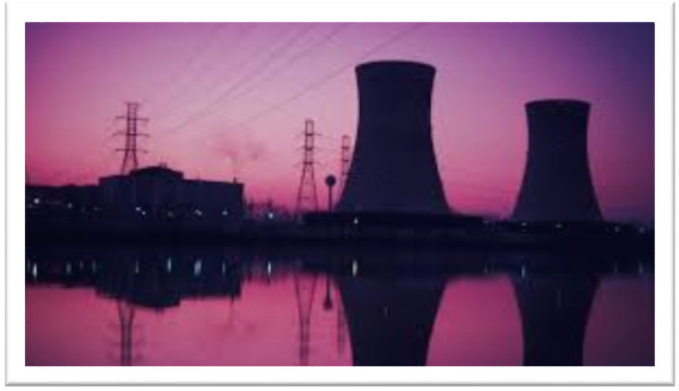
SCADA

- **Système de télégestion à grande échelle**
  - Acquisition de milliers de capteurs
  - Contrôle à distance d'installations techniques

- **Utilisation**
  - Surveillance de processus industriels
  - Transport de produits chimiques
  - Production d'électricité
  - Transport de gaz et de pétrole
  - …

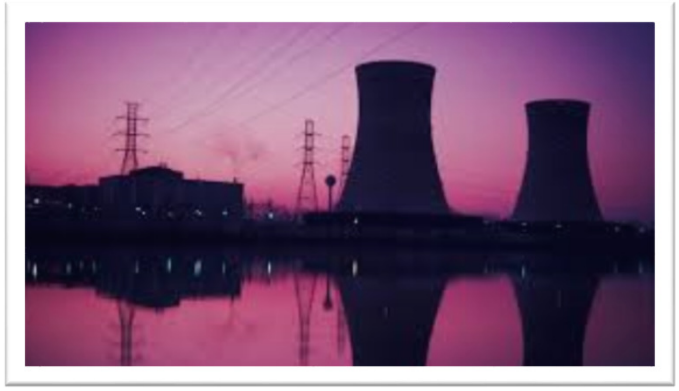
Université Bretagne Sud

Stuxnet (~2010)



- Vers très complexe
  - Capable se propager seul
  - Capable d'échapper aux anti-virus
  - Exploite plusieurs *0-day* inconnues de différentes *.dll* Microsoft (en 2010)

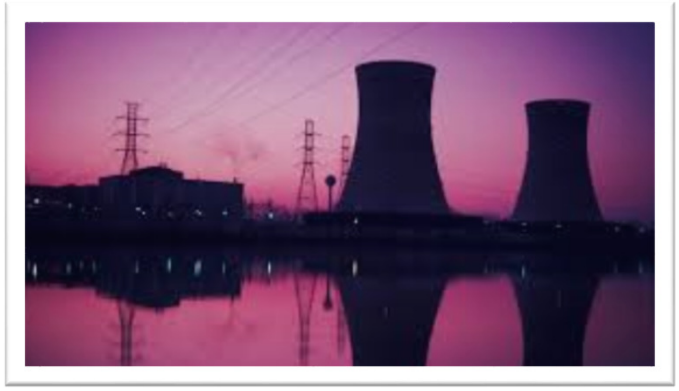
Stuxnet (~2010)



- **Vers très complexe**
  - Capable se propager seul
  - Capable d'échapper aux anti-virus
  - Exploite plusieurs 0-day inconnues de différentes *.dll* Microsoft (en 2010)

  - **S'active lorsque trouve sa cible**
    - **Systèmes SCADA utilisés pour le contrôle commande de procédés industriels**
    - **Centrifugeuses Siemens pour centrales nucléaires**
    - **Installées en Iran (mais aussi en Allemagne, en France…)**

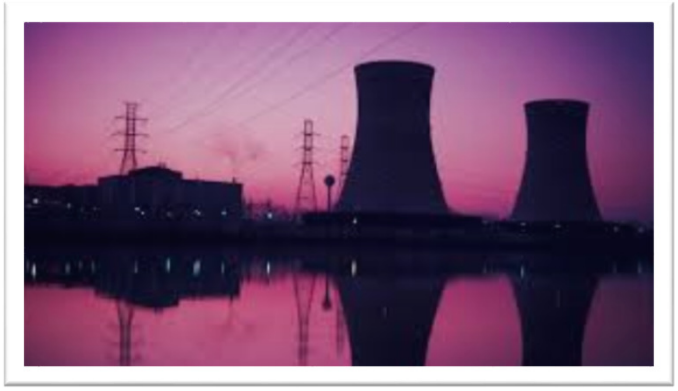
Stuxnet (~2010)



- **Principe**
  - Tromper les ingénieurs pour leur faire croire que tout fonctionne de façon nominal, et en profiter pour mettre en défaut les machines

- **Malware très complexe**
  - Probablement l'œuvre d'un/plusieurs états
  - Implication d'ingénieurs connaissant des détails techniques très pointus
  - …

Stuxnet (~2010)



- **Principe**
  - Tromper les ingénieurs pour leur faire croire que tout fonctionne de façon nominal, et en profiter pour mettre en défaut les machines
- **Malware très complexe**
  - Probablement l'œuvre d'un/plusieurs états
  - Implication d'ingénieurs connaissant des détails techniques très pointus
  - …
- **Nouvelle menace => Industroyer**

Université Bretagne Sud

Duqu (~2011)

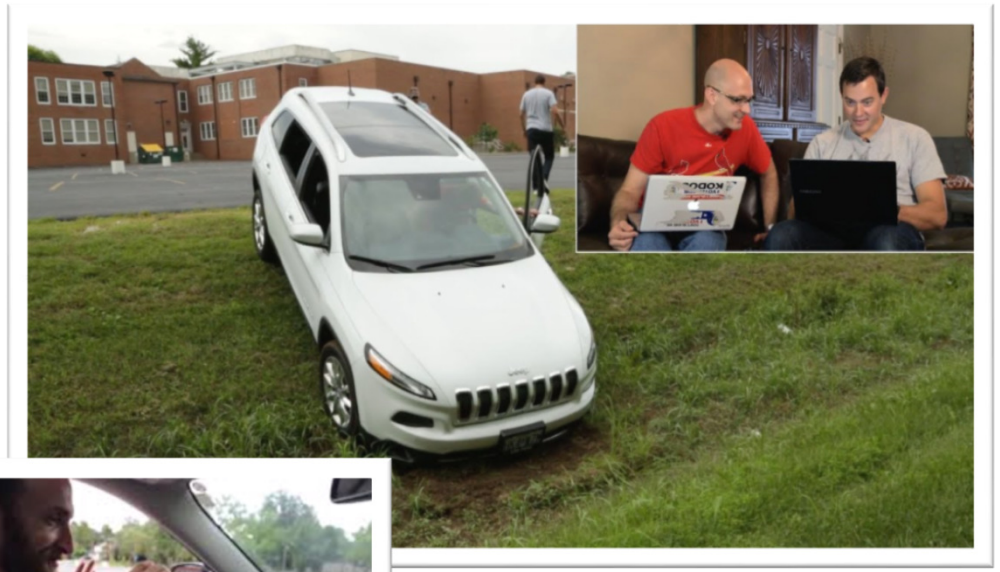
- Vers très proche de Stuxnet
  - Exploite les mêmes failles sur les *.dll*
  - Même mode de propagation
  - Même cible
  - …
  - Même auteur ??

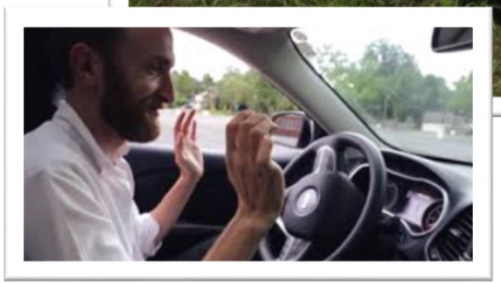
Source: https://cockpitci.itrust.lu/duqu-a-son-of-stuxnext-summary-of-technical-analysis

Université Bretagne Sud

Les voitures connectées

- **Prise contrôle via internet d'une Jeep**
  - **Démonstration de Charlie Miller et Chris Valasek** ***(BlackHat 2015)***

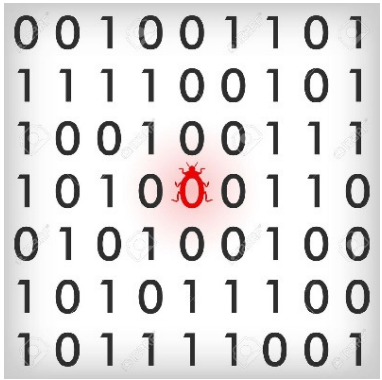




- **Comment ?**
  - **Nombreux services non sécurisés en écoute sur internet**
  - **De nombreuses failles connues exploitables**
  - **Pas de mise à jour du système**
  - **…**

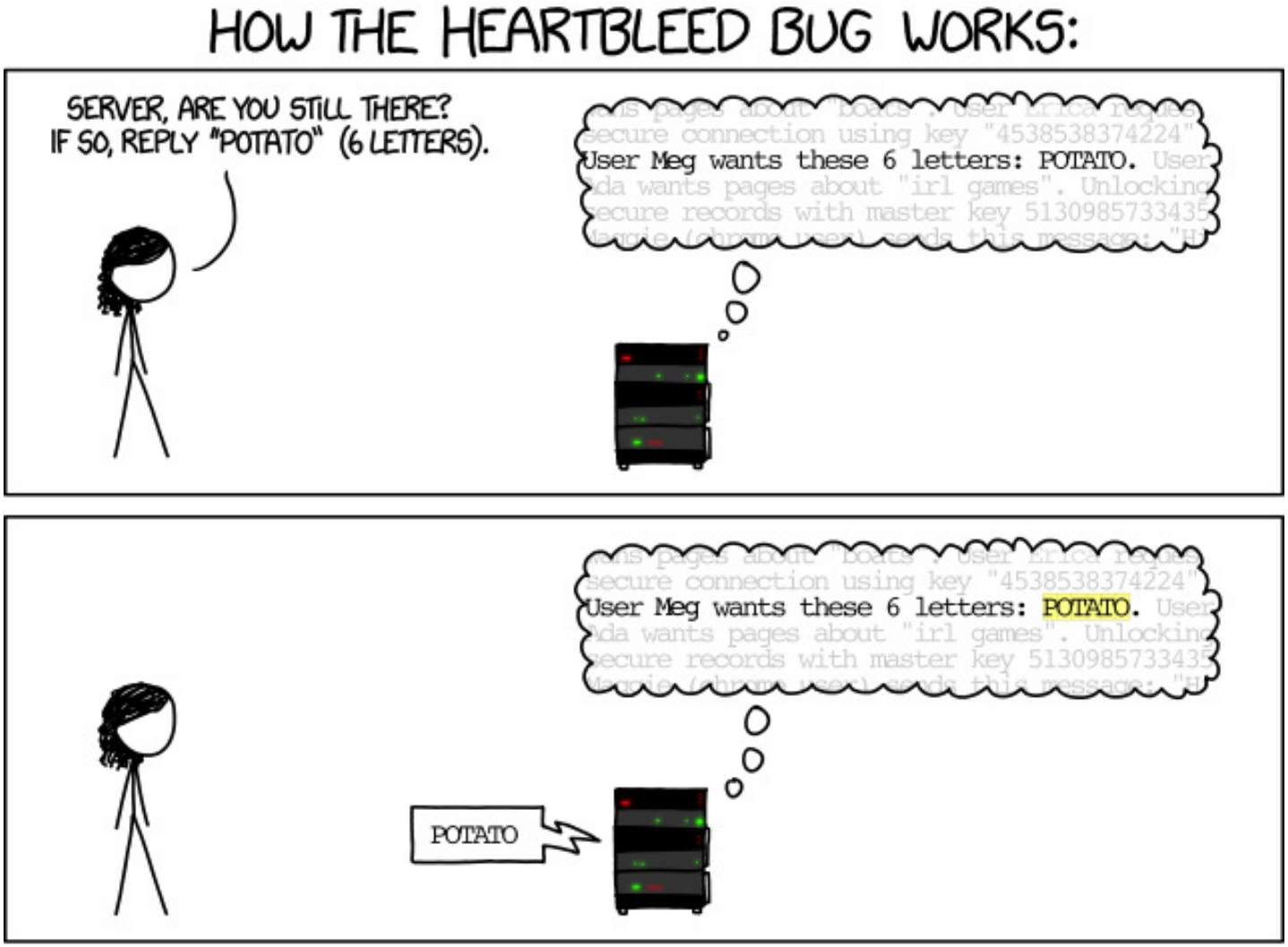
Heartbleed (2014)

- **Fuite de données HTTP**
  - **Accessible à tous**
  - **Bug de codage dans *OpenSSL***
- ***OpenSSL* chiffrement pour HTTPS…**
- **Cause**
  - ***Un simple débordement de tampon***
  - ***Permet de sortir des informations de la mémoire des serveurs…***



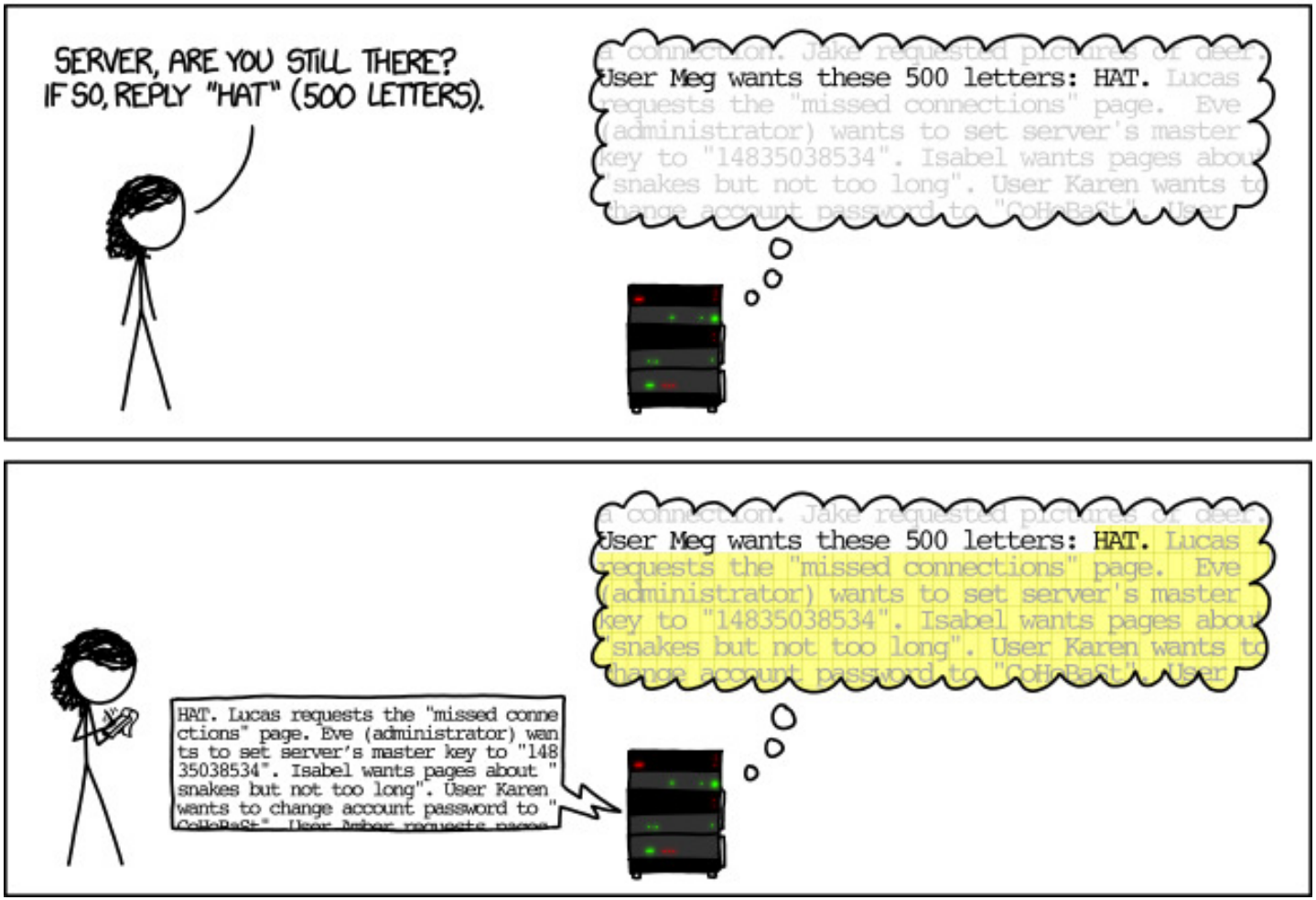
Université Bretagne Sud

Heartbleed (2014)



Source: https://xkcd.com

Heartbleed (2014)



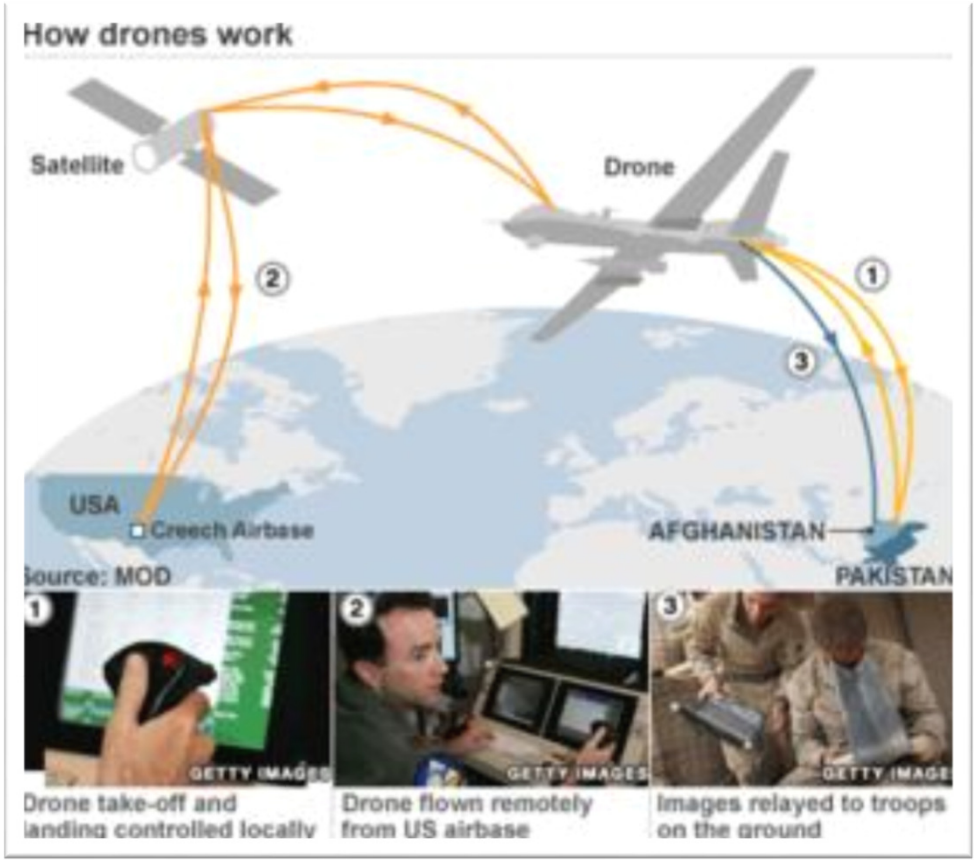
Source: https://xkcd.com

Cyber-Attaque d'un Predator

Université Bretagne Sud

Cyber-Attaque d'un Predator

- **Prise de contrôle par « *spoofing GPS* »**
  - **Attaque ne nécessitant que peu de compétences**
  - **Matériel coûtant entre 500 et 1000 euros**



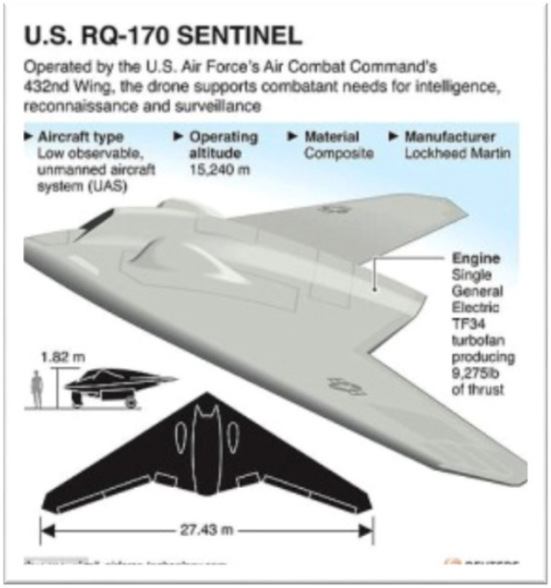
Université Bretagne Sud

Cyber-Attaques d'un Predator

- **Prise de contrôle par « *spoofing GPS* »**
  - **Attaque ne nécessitant que peu de compétences**
  - **Matériel coûtant entre 500 et 1000 euros**
- **Récupération des données transmises par le drone**
  - **Le canal de communication n'était pas chiffré…**

Cyber-Attaques d'un Predator

- **Prise de contrôle par « *spoofing GPS* »**
  - **Attaque ne nécessitant que peu de compétences**
  - **Matériel coûtant entre 500 et 1000 euros**
- **Récupération des données transmises par le drone**
  - **Le canal de communication n'était pas chiffré…**
- **…**



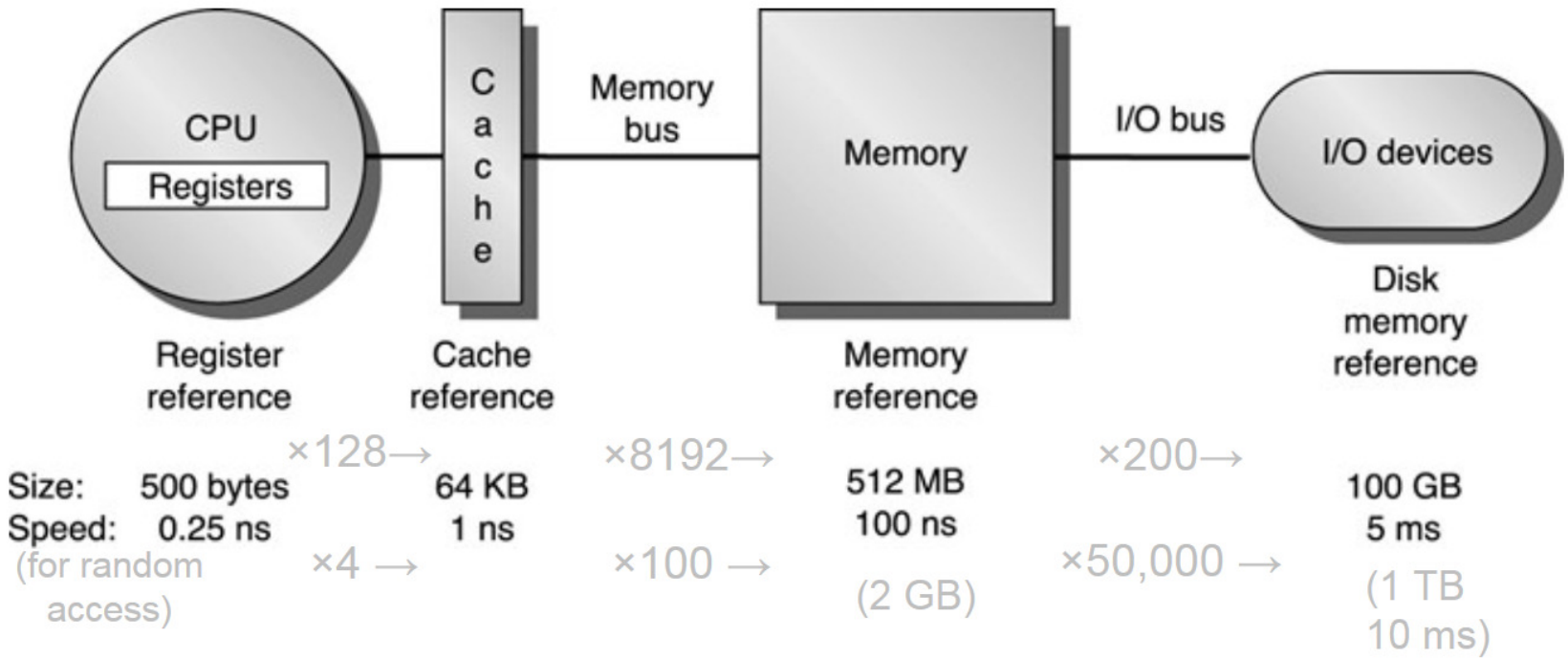
Université Bretagne Sud

Failles matérielles

Source: https://www.howtogeek.com

Failles matérielles

- **Exploit**
  - **Hiérarchie mémoire**
  - **Algorithmes de *prédiction de branchement* des processeurs**



Source: Sherman Anderson

Failles matérielles

	MELTDOWN 	SPECTRE 	FORESHADOW 
Exploit Basis	Attacker must have code running on system	Attacker must have code running on system	Attacker must have code running on system
Processors Affected	Intel, Apple	Intel, AMD, Apple, Arm	Intel (SGX)
Security Impact	Attacker user-space program can read protected kernel memory	Attacker user-space program can read contents of memory from other user's programs	Attacker user-space program can read SGX enclave protected memory and keys

Source: http://www.mellanox.com

Bonnes pratiques

Attention au matériel

- Vous avez trouvé une clef USB ?

Attention au matériel

- Vous avez trouvé une clef USB ?
- Attention elle peut mordre !

Attention au matériel

➢ Souriez-vous êtes filmé !

- Une personne mal intentionnée peut prendre le contrôle de la caméra de votre laptop, PC, smartphone…
- … et vous espionner en toute discrétion !

Université Bretagne Sud

Attention au matériel

➢ Souriez-vous êtes filmé !

- Une personne mal intentionnée peut prendre le contrôle de la caméra de votre laptop, PC, smartphone…
- … et vous espionner en toute discrétion !

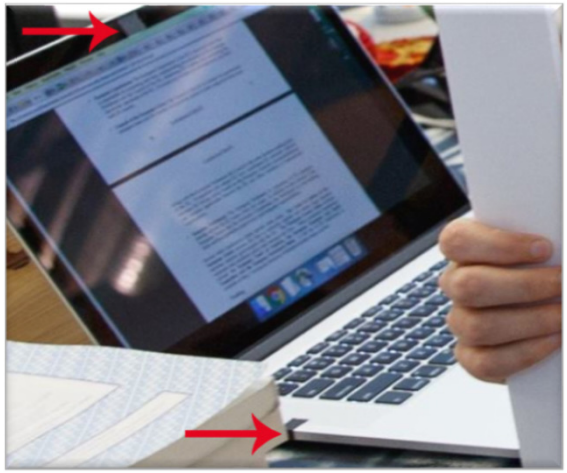
Université Bretagne Sud

Attention au matériel

➢ Souriez-vous êtes filmé !

- Une personne mal intentionnée peut prendre le contrôle de la caméra de votre laptop, PC, smartphone…
- … et vous espionner en toute discrétion !

➢ Solution



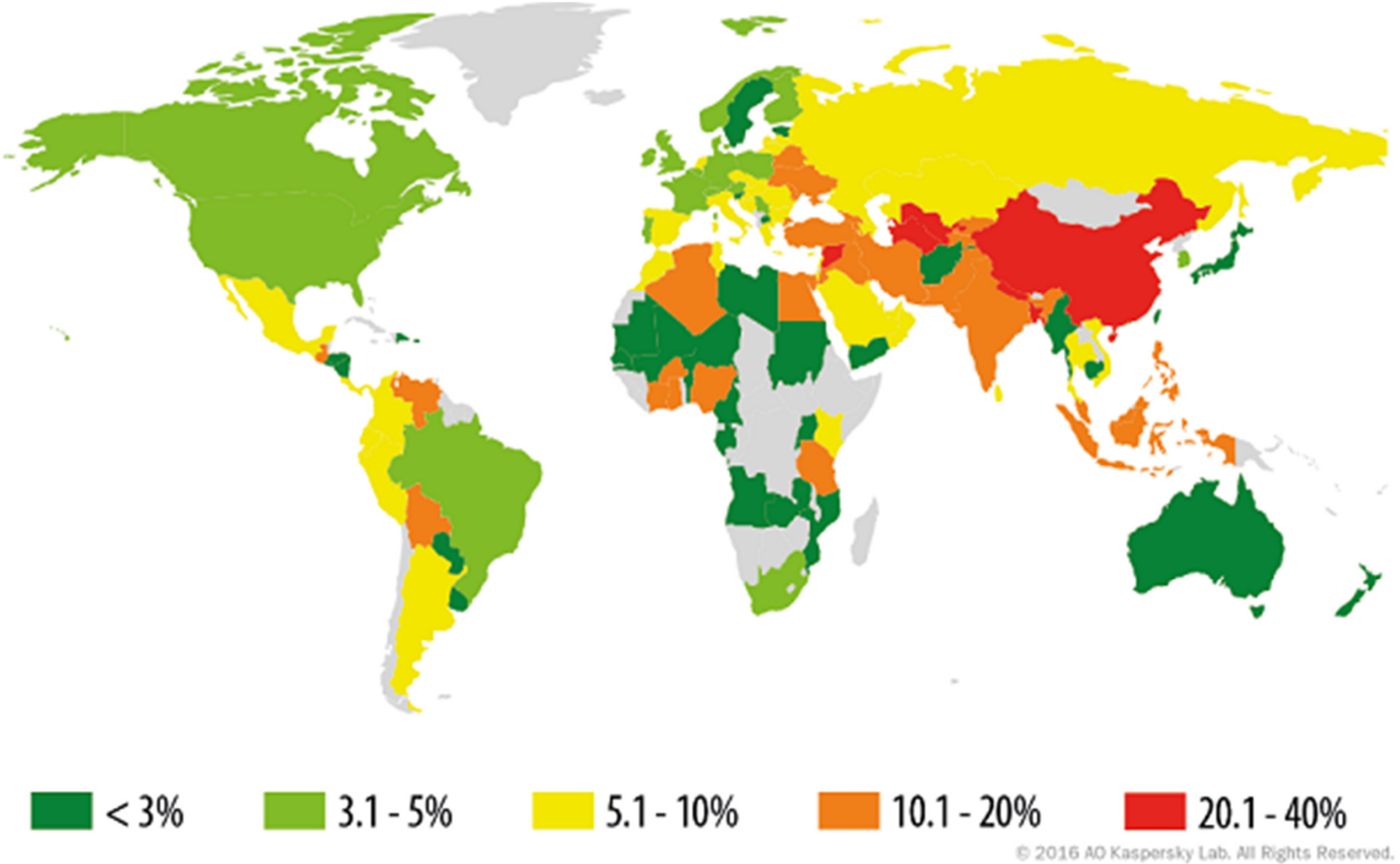
Université Bretagne Sud

Attention aux smartphones

Accelerometer
Gyroscope
Magnetometer
Barometer
Proximity
Amb. Light sensor
Touch screen
Humidity
CO2/VOC gas
Fingerprint

GPS
WiFi
Bluetooth
GSM/CDMA Cell
NFC
Camera (front)
Camera (back)
Colorimeter
Microphones x 3
Thermal ambient

Smartphone attacks



Gestion de vos *logins*

- **Combien de logins utilisez-vous ?**
  - **Facebook, Ebay, Amazon, BlablaCar, SNCF, WhatsAp Instagram, Twitter, GOG, Steam…**
  - **Tablette, smartphone, PC perso, PC pro…**

https://haveibeenpwned.com

Université Bretagne Sud

Gestion de vos *passwords*

- **Combien de mot de passe utilisez-vous ?**
  - **Facebook, Ebay, Amazon, BlablaCar, SNCF, WhatsAp Instagram, Twitter, GOG, Steam, email UBS, email perso, email pro…**
  - **Tablette, smartphone, PC perso, PC pro…**

- **Questions:**
  - **Sont-ils tous différents ?**
  - **Utilisez-vous des mots de passe trop simples ?**
    (123456, azerty, 987654, qwerty, 0000, mot du dictionnaire, date de naissance, mot à l'envers, date…)

Gestion de vos *passwords*

- **Combien de mot de passe utilisez-vous ?**
  - **Facebook, Ebay, Amazon, BlablaCar, SNCF, WhatsAp Instagram, Twitter, GOG, Steam, email UBS, email perso, email pro…**
  - **Tablette, smartphone, PC perso, PC pro…**

- **Questions:**
  - **Sont-ils tous différents ?**
  - **Utilisez-vous des mots de passe trop simples ?**

(123456, azerty, 987654, qwerty, 0000, mot du dictionnaire, date de naissance, mot à l'envers, date…)

Université Bretagne Sud

Gestion de vos *passwords*

- **Solutions possibles**
  - Créer un mot de passe complexe à retenir mais facile à recréer pour **vous**

Gestion de vos *passwords*

➢ Solutions possibles

- Créer un mot de passe complexe à retenir mais facile à recréer pour **vous**

1. Retenez une phrase simple, une citation…
   « Non Luke, je suis ton père !», « Un anneau pour les gouverner tous »

Gestion de vos *passwords*

➢ Solutions possibles

- Créer un mot de passe complexe à retenir mais facile à recréer pour **vous**

1. Retenez une phrase simple, une citation…
   « Non Luke, je suis ton père !», *« Un anneau pour les gouverner tous »*
2. Ne gardez que les première lettres
   NLjstp, ***Uaplgt***

Gestion de vos *passwords*

➢ Solutions possibles

- Créer un mot de passe complexe à retenir mais facile à recréer pour **vous**

1. Retenez une phrase simple, une citation…
   « Non Luke, je suis ton père !», *« Un anneau pour les gouverner tous »*
2. Ne gardez que les première lettres
   NLjstp, *Uaplgt*
3. Changer une lettre par sa position dans l'alphabet
   NLjs20p , ***Uapl7t***

Gestion de vos *passwords*

➢ Solutions possibles

- Créer un mot de passe complexe à retenir mais facile à recréer pour **vous**

1. Retenez une phrase simple, une citation…
   « Non Luke, je suis ton père !», *« Un anneau pour les gouverner tous »*
2. Ne gardez que les première lettres
   NLjstp, *Uaplgt*
3. Changer une lettre par sa position dans l'alphabet
   NLjs20p , *Uapl7t*
4. Changer une lettre par la lettre suivante dans l'alphabet
   NMjs20p , ***Ubpl7t***

Gestion de vos *passwords*

- **Analogie de Chris Pirillo:**

Gestion de vos *passwords*

- **Analogie de Chris Pirillo:**

  « ***Passwords are like underware:***
  you don't let people see it,
  you should change it often,
  and you should never share it with strangers. »

Gestion de vos *passwords*

- **Solutions possibles**
  - Créer un mot de passe complexe à retenir mais facile à recréer pour **vous**
  - Utiliser un gestionnaire de mot de passe

KeePass

LastPass •••|

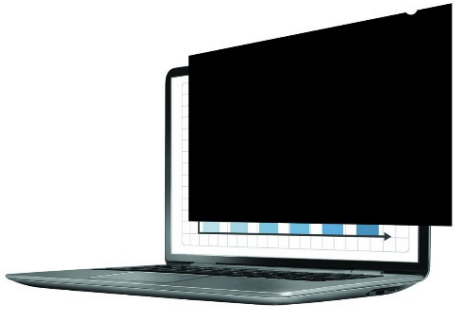
Université Bretagne Sud

Dans les transports

- **Vous travailler dans le bus, le train ou un avion ?**
  - On peut facilement regarder par-dessus votre épaule…

Dans les transports

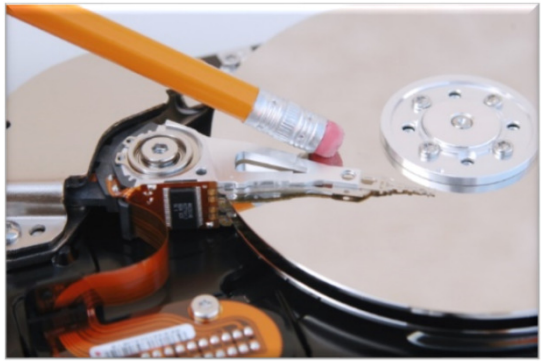
- **Vous travailler dans le bus, le train ou un avion ?**
  - On peut facilement regarder par-dessus votre épaule…
- **Solution**
  - Utiliser un filtre de confidentialité



Annihilation de données

➢ Comment effacer des données sensibles?

- **Vider le disque (disque dur, clefs USB…) et le remplir à nouveau avec des fichiers sans valeur plusieurs fois de suites**



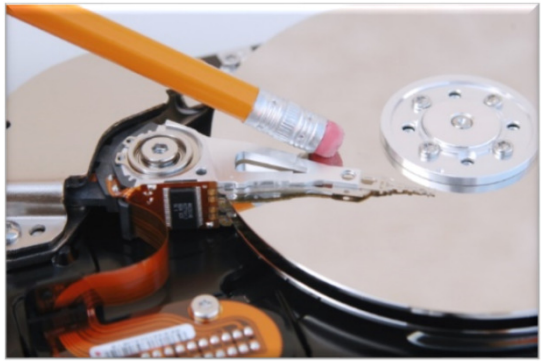
Université Bretagne Sud

Annihilation de données

➢ Comment effacer des données sensibles?

- **Vider le disque (disque dur, clefs USB…) et le remplir à nouveau avec des fichiers sans valeur plusieurs fois de suites**

- **(et/ou) Utiliser des logiciels dédiés**

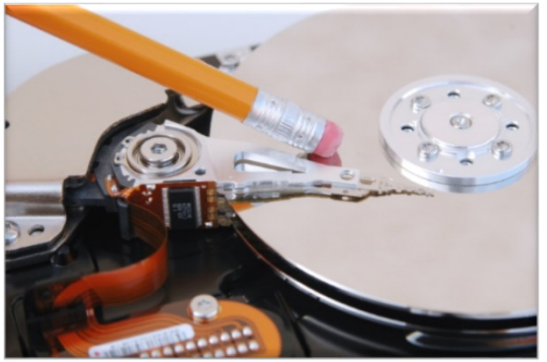


Université Bretagne Sud

Annihilation de données

➢ Comment effacer des données sensibles?

- **Vider le disque (disque dur, clefs USB…) et le remplir à nouveau avec des fichiers sans valeur plusieurs fois de suites**
- **(et/ou) Utiliser des logiciels dédiés**
- **(et) Détruire physiquement le disque**



Université Bretagne Sud

En résumé

- Ne pas utiliser de matériel non certifié par sa DSI
- Ne pas utiliser un mot de passe par défaut, utilisez un gestionnaire de mot de passe

En résumé

- Ne pas utiliser de matériel non certifié par sa DSI
- Ne pas utiliser un mot de passe par défaut, utilisez un gestionnaire de mot de passe
- Ne voyagez pas avec vos outils pro (ou protégez les un ~~minimum~~ **maximum**)

En résumé

- Ne pas utiliser de matériel non certifié par sa DSI
- Ne pas utiliser un mot de passe par défaut, utilisez un gestionnaire de mot de passe
- Ne voyagez pas avec vos outils pro (ou protégez les un ~~minimum~~ **maximum**)
- Les GAFAM ne vous veulent pas que du bien

En résumé

- Ne pas utiliser de matériel non certifié par sa DSI
- Ne pas utiliser un mot de passe par défaut, utilisez un gestionnaire de mot de passe
- Ne voyagez pas avec vos outils pro (ou protégez les un ~~minimum~~ **maximum**)
- Les GAFAM ne vous veulent pas que du bien
- Assurez-vous que votre système est à jour
- Assurez-vous d'avoir un antivirus à jour
- Ne pas se laisser séduire par des emails alléchants (promotion, argent, gloire, sexe…)
  - Si c'est **trop beau pour être vrai** => **DANGER** !

Université Bretagne Sud

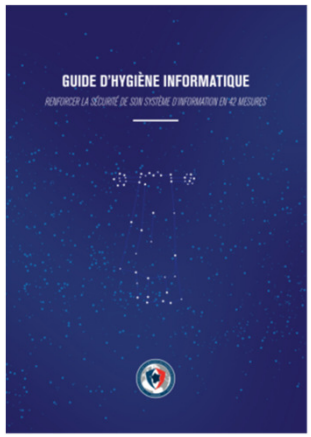
Comment réagir ?

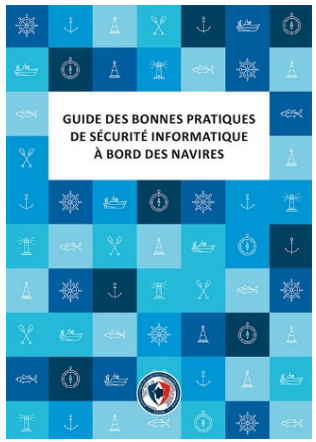
Avoir des réflexes simples

- Faire appel à sa DSI
- Référent ANSSI régional
- Contacter services de police/gendarmerie spécialisés
- Le cas échéant contacter votre banque

Multiples ressources

- **Le site de l'ANSSI**
- **Assistance**
  - https://www.cybermalveillance.gouv.fr
- **MOOC de l'ANSSI**
  - https://secnumacademie.gouv.fr
- **Toutes les ressources gratuites de l'ANSSI**





Les 5 lois de la cyber-sécurité

- **S'il existe une vulnérabilité, elle sera exploitée**

Les 5 lois de la cyber-sécurité

- S'il existe une vulnérabilité, elle sera exploitée
- Tout système est vulnérable d'une façon ou d'une autre

Les 5 lois de la cyber-sécurité

- S'il existe une vulnérabilité, elle sera exploitée
- Tout système est vulnérable d'une façon ou d'une autre
-

Les 5 lois de la cyber-sécurité

- **S'il existe une vulnérabilité, elle sera exploitée**
- **Tout système est vulnérable d'une façon ou d'une autre**
- **Les êtres humains accordent leur confiance facilement, même s'ils ne devraient pas**

Voir les chaines **Hygiène Mentale**, **La tronche en Biais**…

Les 5 lois de la cyber-sécurité

- S'il existe une vulnérabilité, elle sera exploitée
- Tout système est vulnérable d'une façon ou d'une autre
- Les êtres humains accordent leur confiance facilement, même s'ils ne devraient pas
- Les innovations apportent de nouvelles cibles d'exploit

Les 5 lois de la cyber-sécurité

- S'il existe une vulnérabilité, elle sera exploitée
- Tout système est vulnérable d'une façon ou d'une autre
- Les êtres humains accordent leur confiance facilement, même s'ils ne devraient pas
- Les innovations apportent de nouvelles cibles d'exploit
- En cas de doute, voir la première loi

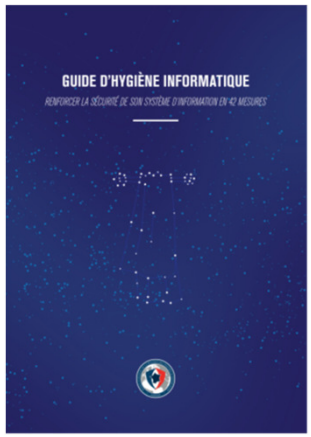
Université Bretagne Sud

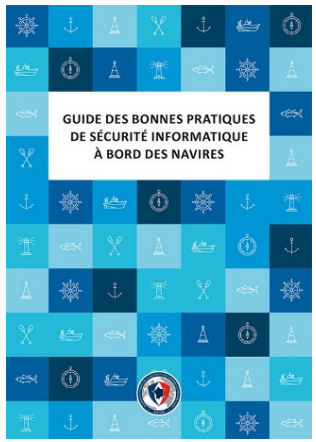
Last *(but not least)*

- **Que vous soyez concepteur, développeur ou simple utilisateur…**

Soyez paranoïaques !

There is not patch for stupidity !!





Université Bretagne Sud

Sécurité des Systèmes d'Information

Introduction & Bonnes pratiques

Dr. Cyrille CHAVET

Université Bretagne Sud

Lab-STICC

www.univ-ubs.fr

Back up