

CyberEdu : pourquoi et comment parler de sécurité du numérique

Olivier Levillain

Agence nationale de la sécurité de systèmes d'information
Association CyberEdu

19 juin 2018

Plan

Enjeux de la sécurité : quelques exemples

La démarche CyberEdu et l'esprit sécurité

Plan

Enjeux de la sécurité : quelques exemples

La démarche CyberEdu et l'esprit sécurité

MS17-010 : la menace des rançongiciels



En mai et juin 2017, deux attaques très médiatisées sur des rançongiciels

- ▶ exploitation d'une vulnérabilité critique dans Windows
- ▶ ... sur un service qui ne devrait pas être exposé
- ▶ ... pour lequel un correctif est disponible depuis mars

MS17-010 : la menace des rançongiciels



En mai et juin 2017, deux attaques très médiatisées sur des rançongiciels

- ▶ exploitation d'une vulnérabilité critique dans Windows
- ▶ ... sur un service qui ne devrait pas être exposé
- ▶ ... pour lequel un correctif est disponible depuis mars
- ▶ pourquoi la sécurité semble-t-elle un échec ?

Une voiture connectée



Charlie Miller et Chris Valasek (BlackHat2015) : prise de contrôle à distance d'une Jeep

- ▶ Cause : de nombreux services non sécurisés en écoute sur internet

Une voiture connectée



Charlie Miller et Chris Valasek (BlackHat2015) : prise de contrôle à distance d'une Jeep

- ▶ Cause : de nombreux services non sécurisés en écoute sur internet
- ▶ Combien de voitures (avions, usines...) reposent de manière critique sur du logiciel pour fonctionner ?

Heartbleed



Heartbleed (8 avril 2014)

- ▶ Fuite de données HTTP accessibles à tous de manière discrète
- ▶ Une faille très médiatisée
- ▶ Cause : un débordement de tampon dans OpenSSL...

Heartbleed



Heartbleed (8 avril 2014)

- ▶ Fuite de données HTTP accessibles à tous de manière discrète
- ▶ Une faille très médiatisée
- ▶ Cause : un débordement de tampon dans OpenSSL...
- ▶ ... dans une fonctionnalité inutilisée (mais activée par défaut)

Heartbleed



Heartbleed (8 avril 2014)

- ▶ Fuite de données HTTP accessibles à tous de manière discrète
- ▶ Une faille très médiatisée
- ▶ Cause : un débordement de tampon dans OpenSSL...
- ▶ ... dans une fonctionnalité inutilisée (mais activée par défaut)
- ▶ ... qui permet de récupérer des bouts de la mémoire du serveur

Heartbleed



Heartbleed (8 avril 2014)

- ▶ Fuite de données HTTP accessibles à tous de manière discrète
- ▶ Une faille très médiatisée
- ▶ Cause : un débordement de tampon dans OpenSSL...
- ▶ ... dans une fonctionnalité inutilisée (mais activée par défaut)
- ▶ ... qui permet de récupérer des bouts de la mémoire du serveur
- ▶ Connaissez-vous l'autre information SSI du 8 avril 2014 ?

Stuxnet



(Source : Office of the Presidency of the Islamic Republic of Iran)

Attaque de systèmes industriels (centrifugeuses) en Iran (2010)

- ▶ Manipulation du logiciel des automates pour saboter les équipements...
- ▶ ... tout en remontant des informations fausses à la supervision

Stuxnet



(Source : Office of the Presidency of the Islamic Republic of Iran)

Attaque de systèmes industriels (centrifugeuses) en Iran (2010)

- ▶ Manipulation du logiciel des automates pour saboter les équipements...
- ▶ ... tout en remontant des informations fausses à la supervision
- ▶ Cause : des logiciels propriétaires sans aucune défense
 - ▶ limites de la sécurité par l'obscurité

Stuxnet



(Source : Office of the Presidency of the Islamic Republic of Iran)

Attaque de systèmes industriels (centrifugeuses) en Iran (2010)

- ▶ Manipulation du logiciel des automates pour saboter les équipements...
- ▶ ... tout en remontant des informations fausses à la supervision
- ▶ Cause : des logiciels propriétaires sans aucune défense
 - ▶ limites de la sécurité par l'obscurité
- ▶ Les installations en question étaient sur un réseau dédié
 - ▶ limites de l'*air gap*

Santé et sécurité

Les *pacemakers* ont aujourd'hui des interfaces sans fil pour permettre un suivi en temps réel des patients

- ▶ Dick Cheney (vice-président des USA sous Georges W. Bush) a été convaincu par la NSA de désactiver ces interfaces
- ▶ Quelques publications académiques sur le sujet

Santé et sécurité

Les *pacemakers* ont aujourd'hui des interfaces sans fil pour permettre un suivi en temps réel des patients

- ▶ Dick Cheney (vice-président des USA sous Georges W. Bush) a été convaincu par la NSA de désactiver ces interfaces
- ▶ Quelques publications académiques sur le sujet
- ▶ Scénario utilisé dans une série américaine

Santé et sécurité

Les *pacemakers* ont aujourd'hui des interfaces sans fil pour permettre un suivi en temps réel des patients

- ▶ Dick Cheney (vice-président des USA sous Georges W. Bush) a été convaincu par la NSA de désactiver ces interfaces
- ▶ Quelques publications académiques sur le sujet
- ▶ Scénario utilisé dans une série américaine

Erreurs logicielles et santé

- ▶ Erreur de calcul dans les doses de radiation à Epinal

Santé et sécurité

Les *pacemakers* ont aujourd'hui des interfaces sans fil pour permettre un suivi en temps réel des patients

- ▶ Dick Cheney (vice-président des USA sous Georges W. Bush) a été convaincu par la NSA de désactiver ces interfaces
- ▶ Quelques publications académiques sur le sujet
- ▶ Scénario utilisé dans une série américaine

Erreurs logicielles et santé

- ▶ Erreur de calcul dans les doses de radiation à Epinal

L'informatique s'imisce de plus en plus dans le monde *réel*

Les caméras à l'assaut d'OVH

En septembre 2016, un réseau de caméras infectées par un logiciel malveillant (un *botnet*) a servi à monter plusieurs attaques DDoS

- ▶ DDoS = *Distributed Denial of Service*
- ▶ La bande passante reçue par OVH a été estimée à 1 Tbps

Les caméras à l'assaut d'OVH

En septembre 2016, un réseau de caméras infectées par un logiciel malveillant (un *botnet*) a servi à monter plusieurs attaques DDoS

- ▶ DDoS = *Distributed Denial of Service*
- ▶ La bande passante reçue par OVH a été estimée à 1 Tbps

Les causes de l'attaque

- ▶ de nombreux équipements connectés avec des mots de passe connus
- ▶ les caméras ont souvent une bonne connectivité

Les caméras à l'assaut d'OVH

En septembre 2016, un réseau de caméras infectées par un logiciel malveillant (un *botnet*) a servi à monter plusieurs attaques DDoS

- ▶ DDoS = *Distributed Denial of Service*
- ▶ La bande passante reçue par OVH a été estimée à 1 Tbps

Les causes de l'attaque

- ▶ de nombreux équipements connectés avec des mots de passe connus
- ▶ les caméras ont souvent une bonne connectivité

Pour aller plus loin

- ▶ un précédent intéressant : l'Internet Census 2012...
- ▶ au fait, qui est responsable ?

La sécurité du numérique : un sujet omniprésent

Que nous apprennent ces exemples

- ▶ les systèmes informatiques...
- ▶ ... sont omniprésents
- ▶ ... sont complexes
- ▶ ... ont un impact sur le monde physique
- ▶ ... et sur des vies humaines

La sécurité du numérique : un sujet omniprésent

Que nous apprennent ces exemples

- ▶ les systèmes informatiques...
- ▶ ... sont omniprésents
- ▶ ... sont complexes
- ▶ ... ont un impact sur le monde physique
- ▶ ... et sur des vies humaines

Comment les protéger face aux menaces nombreuses et variées ?

La sécurité du numérique : un sujet omniprésent

Que nous apprennent ces exemples

- ▶ les systèmes informatiques...
- ▶ ... sont omniprésents
- ▶ ... sont complexes
- ▶ ... ont un impact sur le monde physique
- ▶ ... et sur des vies humaines

Comment les protéger face aux menaces nombreuses et variées ?

Au-delà des spécialistes, il faut former et responsabiliser les acteurs des systèmes d'information

Quelques réponses

La sécurité du numérique est l'affaire de tous

- ▶ les spécialistes doivent protéger et défendre les systèmes
 - ▶ SecNumedu
 - ▶ guides techniques de l'ANSSI

Quelques réponses

La sécurité du numérique est l'affaire de tous

- ▶ les spécialistes doivent protéger et défendre les systèmes
 - ▶ SecNumedu
 - ▶ guides techniques de l'ANSSI
- ▶ les acteurs du système d'information doivent acquérir de bons réflexes pour rendre le travail des spécialistes possibles
 - ▶ CyberEdu
 - ▶ le guide d'hygiène

Quelques réponses

La sécurité du numérique est l'affaire de tous

- ▶ les spécialistes doivent protéger et défendre les systèmes
 - ▶ *SecNumedu*
 - ▶ guides techniques de l'ANSSI
- ▶ les acteurs du système d'information doivent acquérir de bons réflexes pour rendre le travail des spécialistes possibles
 - ▶ CyberEdu
 - ▶ le guide d'hygiène
- ▶ l'ensemble des utilisateurs doit être sensibilisés
 - ▶ *SecNumacadémie*
 - ▶ ACYMA et cybermalveillance.gouv.fr

Un peu d'hygiène informatique



Morceaux choisis

- ▶ cartographier son système d'information
- ▶ mettre à jour régulièrement vos logiciels
- ▶ choisir avec soin ses mots de passe
- ▶ effectuer des sauvegardes régulières
- ▶ être prudent lors de l'usage de sa messagerie



Plan

Enjeux de la sécurité : quelques exemples

La démarche CyberEdu et l'esprit sécurité

CyberEdu en quelques mots

Quelques constats :

- ▶ obtenir un niveau de sécurité acceptable est difficile
- ▶ un expert en SSI ne peut rien face à une horde de développeurs/administrateurs non sensibilisés
- ▶ la sécurité est l'affaire de tous !

CyberEdu en quelques mots

Quelques constats :

- ▶ obtenir un niveau de sécurité acceptable est difficile
- ▶ un expert en SSI ne peut rien face à une horde de développeurs/administrateurs non sensibilisés
- ▶ la sécurité est l'affaire de tous !

Démarche

- ▶ inciter et accompagner l'intégration de la SSI dans les formations du supérieur en informatique
- ▶ intérêt pédagogique
- ▶ intérêt *marketing*

CyberEdu : quelques exemples concrets

CyberEdu : quelques exemples concrets

- ▶ Un administrateur réseau doit savoir que l'on peut changer l'adresse MAC d'une carte réseau

CyberEdu : quelques exemples concrets

- ▶ Un administrateur réseau doit savoir que l'on peut changer l'adresse MAC d'une carte réseau
- ▶ Un développeur C doit savoir ce qu'est un *buffer overflow*

CyberEdu : quelques exemples concrets

- ▶ Un administrateur réseau doit savoir que l'on peut changer l'adresse MAC d'une carte réseau
- ▶ Un développeur C doit savoir ce qu'est un *buffer overflow*
- ▶ Un admin sys doit savoir comment sont stockés les mots de passe

CyberEdu : quelques exemples concrets

- ▶ Un administrateur réseau doit savoir que l'on peut changer l'adresse MAC d'une carte réseau
- ▶ Un développeur C doit savoir ce qu'est un *buffer overflow*
- ▶ Un admin sys doit savoir comment sont stockés les mots de passe
- ▶ Un développeur web doit savoir ce qu'est une injection SQL

CyberEdu : quelques exemples concrets

- ▶ Un administrateur réseau doit savoir que l'on peut changer l'adresse MAC d'une carte réseau
- ▶ Un développeur C doit savoir ce qu'est un *buffer overflow*
- ▶ Un admin sys doit savoir comment sont stockés les mots de passe
- ▶ Un développeur web doit savoir ce qu'est une injection SQL
- ▶ Un informaticien doit savoir ce qu'est un certificat électronique

Qu'est-ce que la sécurité? (1/2)

Parmi les commandes suivantes, lesquelles sont susceptibles (sans redirection) de provoquer la destruction des données d'un fichier?

- `ls` `cd` `cp` `cat` `rm` `mv`

Qu'est-ce que la sécurité? (1/2)

Parmi les commandes suivantes, lesquelles sont susceptibles (sans redirection) de provoquer la destruction des données d'un fichier?

- `ls` `cd` `cp` `cat` `rm` `mv`

Fonctionnel

- ▶ Question ré-interprétée « *Comment détruire les données d'un fichier?* », seule la commande `rm` est mentionnée

Qu'est-ce que la sécurité? (1/2)

Parmi les commandes suivantes, lesquelles sont susceptibles (sans redirection) de provoquer la destruction des données d'un fichier?

- `ls` `cd` `cp` `cat` `rm` `mv`

Fonctionnel

- ▶ Question ré-interprétée « *Comment détruire les données d'un fichier?* », seule la commande `rm` est mentionnée

Sécurité

- ▶ Si on cherche à protéger les données, les commandes dangereuses sont `rm` mais aussi `cp` et `mv`, qui écrasent les fichiers cibles

Qu'est-ce que la sécurité? (2/2)

Spécification de deux fonctions pour la compression (Zip) et la décompression (Unzip) de fichiers

Qu'est-ce que la sécurité? (2/2)

Spécification de deux fonctions pour la compression (Zip) et la décompression (Unzip) de fichiers

Fonctionnel

- ▶ $\forall (f : \text{File}), \text{Unzip}(\text{Zip } f) = f$

Qu'est-ce que la sécurité? (2/2)

Spécification de deux fonctions pour la compression (Zip) et la décompression (Unzip) de fichiers

Fonctionnel

- ▶ $\forall (f : \text{File}), \text{Unzip}(\text{Zip } f) = f$

Sécurité

- ▶ $\forall (c : \text{File}), (\neg \exists (f : \text{File}), \text{Zip } f = c) \Rightarrow \text{Unzip } c = \text{Error}$
- ▶ En particulier, ne pas faire confiance à un champ annonçant à l'avance la taille du fichier décompressé

L'esprit de sécurité

Comment résumer cet état d'esprit nécessaire pour « penser sécurité » ?

L'esprit de sécurité

Comment résumer cet état d'esprit nécessaire pour « penser sécurité » ?

- ▶ il faut penser *au-delà du fonctionnel*

L'esprit de sécurité

Comment résumer cet état d'esprit nécessaire pour « penser sécurité » ?

- ▶ il faut penser *au-delà du fonctionnel*
- ▶ pour défendre, il faut couvrir tous les chemins d'attaques possibles de manière cohérente (principe du maillon faible)

L'esprit de sécurité

Comment résumer cet état d'esprit nécessaire pour « penser sécurité » ?

- ▶ il faut penser *au-delà du fonctionnel*
- ▶ pour défendre, il faut couvrir tous les chemins d'attaques possibles de manière cohérente (principe du maillon faible)
- ▶ aucune défense n'est parfaite, il faut combiner des mécanismes pour créer des lignes de défense multiples et complémentaires (principe de la défense en profondeur)

L'esprit de sécurité

Comment résumer cet état d'esprit nécessaire pour « penser sécurité » ?

- ▶ il faut penser *au-delà du fonctionnel*
- ▶ pour défendre, il faut couvrir tous les chemins d'attaques possibles de manière cohérente (principe du maillon faible)
- ▶ aucune défense n'est parfaite, il faut combiner des mécanismes pour créer des lignes de défense multiples et complémentaires (principe de la défense en profondeur)
- ▶ de manière générale, en sécurité, on se pose beaucoup de questions...

L'esprit de sécurité

Comment résumer cet état d'esprit nécessaire pour « penser sécurité » ?

- ▶ il faut penser *au-delà du fonctionnel*
- ▶ pour défendre, il faut couvrir tous les chemins d'attaques possibles de manière cohérente (principe du maillon faible)
- ▶ aucune défense n'est parfaite, il faut combiner des mécanismes pour créer des lignes de défense multiples et complémentaires (principe de la défense en profondeur)
- ▶ de manière générale, en sécurité, on se pose beaucoup de questions...
- ▶ sans pouvoir apporter de réponses génériques valables à tous les coups (d'où l'importance du contexte et d'une analyse de risque)

Quelques grands principes de sécurité

- ▶ La complexité est l'ennemi de la sécurité
 - ▶ on parle souvent de réduction de la surface d'attaque
 - ▶ exemple de loupé : Heartbleed

Quelques grands principes de sécurité

- ▶ La complexité est l'ennemi de la sécurité
 - ▶ on parle souvent de réduction de la surface d'attaque
 - ▶ exemple de loupé : Heartbleed

- ▶ La défense en profondeur
 - ▶ prévenir
 - ▶ bloquer
 - ▶ contenir
 - ▶ détecter
 - ▶ réparer

2013 – 2016 : lancement de CyberEdu par l'ANSSI

Deux grandes réalisations

- ▶ un appel d'offres pour la fourniture d'un guide pédagogique et de supports de cours
- ▶ organisation de colloques de 3 jours à l'ANSSI au profit des formateurs

Supports pédagogiques (licence CC-BY)

- ▶ un guide pédagogique
- ▶ des planches de présentation pour un module de sensibilisation d'environ 20 heures
- ▶ des fiches pédagogiques sur différents sujets

Limites de la première phase

Pour aller plus loin, il était nécessaire

- ▶ d'associer durablement les enseignants à la démarche
- ▶ d'éviter le tropisme parisien des activités proposées

Limites de la première phase

Pour aller plus loin, il était nécessaire

- ▶ d'associer durablement les enseignants à la démarche
- ▶ d'éviter le tropisme parisien des activités proposées

Une première communauté : les participants aux colloques

- ▶ cinq sessions
- ▶ plus d'une centaine de personnes
- ▶ ... venues de toute la France

Depuis 2016 : l'association

L'association CyberEdu

- ▶ création en mai 2016
- ▶ ses membres sont des enseignants-chercheurs
- ▶ ... répartis sur tout le territoire métropolitain

Depuis 2016 : l'association

L'association CyberEdu

- ▶ création en mai 2016
- ▶ ses membres sont des enseignants-chercheurs
- ▶ ... répartis sur tout le territoire métropolitain

Missions

- ▶ maintenir à jour les documents existants et en proposer de nouveaux
- ▶ proposer des colloques sur l'ensemble du territoire
- ▶ offrir un forum d'échanges entre spécialistes et non spécialistes de la sécurité
- ▶ labelliser des formations « CyberEdu »
- ▶ étendre son périmètre
 - ▶ au-delà des formations en informatique
 - ▶ au-delà des formations initiales

Premier bilan

Colloques

- ▶ journée sur le développement à Poitiers en décembre
- ▶ journée à Nantes en avril
- ▶ journée à Colmar en juin
- ▶ CyberEdu, bientôt près de chez vous !

Premier bilan

Colloques

- ▶ journée sur le développement à Poitiers en décembre
- ▶ journée à Nantes en avril
- ▶ journée à Colmar en juin
- ▶ CyberEdu, bientôt près de chez vous !

Label CyberEdu

- ▶ référencement par l'association des formations intégrant des contenus de sensibilisation
- ▶ premiers labels en novembre 2017
- ▶ gros retard actuellement sur les dossiers

Premier bilan

Colloques

- ▶ journée sur le développement à Poitiers en décembre
- ▶ journée à Nantes en avril
- ▶ journée à Colmar en juin
- ▶ CyberEdu, bientôt près de chez vous !

Label CyberEdu

- ▶ référencement par l'association des formations intégrant des contenus de sensibilisation
- ▶ premiers labels en novembre 2017
- ▶ gros retard actuellement sur les dossiers

Extension à la formation continue

- ▶ convention avec l'Afpa fin octobre
- ▶ intégration de compétences sécurité dans les titres professionnels en informatique

Conclusion

- ▶ La sécurité n'est pas uniquement l'affaire des spécialistes
- ▶ CyberEdu a pour objectif d'injecter de la sécurité dans les formations du supérieur en informatique (et au-delà)
- ▶ Plus d'information sur <https://www.cyberedu.fr>

Questions ?

Merci de votre attention

`olivier.levillain@ssi.gouv.fr`



<https://www.cyberedu.fr>