CyberEdu : pourquoi et comment parler de sécurité du numérique

Olivier Levillain

Agence nationale de la sécurité de systèmes d'information

30 juin 2017

Plan

Plan

Qui suis-je ?

Olivier Levillain (@pictyeye)

Qui suis-je ?

Olivier Levillain (@pictyeye)

- stage de DEA en cryptographie sur une fonction de hachage
- membre du laboratoire « système » de l'ANSSI (2007-2012)
- responsable du laboratoire « réseau » de l'ANSSI (2012-2015)
- responsable du CFSSI, centre de formation de l'ANSSI (2015-)

Qui suis-je ?

Olivier Levillain (@pictyeye)

- stage de DEA en cryptographie sur une fonction de hachage
- membre du laboratoire « système » de l'ANSSI (2007-2012)
- responsable du laboratoire « réseau » de l'ANSSI (2012-2015)
- responsable du CFSSI, centre de formation de l'ANSSI (2015-)

Recherche

- participation aux travaux sur les mécanismes bas-niveau x86
- études sur les langages depuis 2007
- travaux sur SSL/TLS (thèse soutenue en 2016)
- travaux sur les *parsers*

Qui suis-je ?

Olivier Levillain (@pictyeye)

- stage de DEA en cryptographie sur une fonction de hachage
- membre du laboratoire « système » de l'ANSSI (2007-2012)
- responsable du laboratoire « réseau » de l'ANSSI (2012-2015)
- responsable du CFSSI, centre de formation de l'ANSSI (2015-)

Recherche

- participation aux travaux sur les mécanismes bas-niveau x86
- études sur les langages depuis 2007
- travaux sur SSL/TLS (thèse soutenue en 2016)
- travaux sur les *parsers*

Enseignement

- cryptographie : fonctions de hachage et cryptanalyse
- module système pour la formation ESSI
- cours sur SSL/TLS, et plus récemment sur le développement

Présentation rapide de l'ANSSI

- L'Agence Nationale de la Sécurité des Systèmes d'Information, créée en 2009 pour remplacer la DCSSI
- L'ANSSI est rattachée au SGDSN, qui dépend du Premier Ministre
- Effectifs : environ 500 personnes aujourd'hui
- 4 sous-directions métier : RELEC, SIS, COSSI, SDE
- SDE contient la division scientifique et technique, avec notamment cinq laboratoires et le centre de formation

Plan

MS17-010 : Une envie de pleurer ?

Depuis mai, deux attaques très médiatisées sur des rançongiciels

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

MS17-010 : Une envie de pleurer ?

Depuis mai, deux attaques très médiatisées sur des rançongiciels

- exploitation d'une vulnérabilité critiquedans 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 ?
- avantage et inconvénients de la médiatisation

Une voiture connectée

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

- Cause : plein de 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 : plein de 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
- 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
- Nombreux problèmes d'IHM dans les pompes médicales

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 ?

Plan

Le CFSSI (1/2)

Un centre de formation pour l'administration

- activité principale : dispenser à Paris des cours aux fonctionnaires et aux militaires français
- aucun formateur en propre
- les cours sont intégralement dispensés par des vacataires (appartenant à 80 % à l'ANSSI)

Le CFSSI (1/2)

Un centre de formation pour l'administration

- activité principale : dispenser à Paris des cours aux fonctionnaires et aux militaires français
- aucun formateur en propre
- les cours sont intégralement dispensés par des vacataires (appartenant à 80 % à l'ANSSI)

Catalogue de formations

- une vingtaine de stages « courts » (1500 pers./an)
  - 1 : panorama de la SSI (1 jour)
  - 8a : organisation des audits (2 jours)
  - 10 : cryptologie (20 jours)
  - 14 : traitement d'incidents (3-4 jours)
- une formation longue menant au titre ESSI (10 pers./an)
  - une vision technique et large de la sécurité
  - la curiosité et la rigueur comme principes
  - la capacité à conseiller et convaincre comme objectif

Le CFSSI (2/2)

Depuis 2013, extension du domaine d'action du CFSSI

- CyberEdu : sensibiliser à la sécurité du numérique tous les informaticiens de demain
- SecNum*edu* : labelliser les formations de spécialistes en sécurité du numérique
- SecNum*académie* : des modules de sensibilisation en ligne

Plan

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 *marketting*

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

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

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

Livrables (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

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 »

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 »

`https://www.cyberedu.fr`

Rejoignez-nous !

Conclusion

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

Questions ?

Merci de votre attention.

olivier.levillain@ssi.gouv.fr