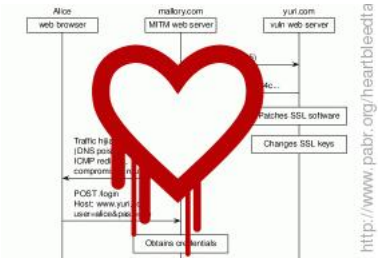
Taxonomie des attaques Heartbleed

Une semaine après l'annonce de la faille "Heartbleed", les experts en sécurité continuent à découvrir ses conséquences pour la sécurité sur Internet. Ce document recense les scénarios d'attaque et les contre-mesures correspondantes. Il vous aidera à comprendre si vous devez vraiment changer vos mots de passe, pourquoi il ne fallait pas le faire trop tôt, et pourquoi vous devez savoir si votre navigateur détecte les certificats révoqués.



READ THE HYPERTEXT VERSION HERE:
http://www.pabr.org/heartbleedtax/heartbleedtax.fr.html

Historique des versions		
1.5	2014-05-08	Ajout vote électronique. Correction DNSSEC.
1.4	2014-04-22	Débat sur la gestion des certificats révoqués.
1.3	2014-04-21	Ajouté services cachés Tor, proxys HTTPS.
1.2	2014-04-19	Ajouté serveur VPN. Références.
1.1	2014-04-18	Ajouté corrélation de trafic Tor. Version française.
1.0	2014-04-16	Première publication.

Table des matières

1. Contexte 3
2. Notations 3
3. Scénarios d'attaques et contre-mesures 4
    3.1. Extraction de données sensible depuis un serveur HTTPS vulnérable 4
    3.2. Extraction de données d'authentification depuis un serveur HTTPS vulnérable 4
    3.3. Détournement de session sur un serveur HTTPS vulnérable 5
    3.4. Extraction de la clé privée SSL d'un serveur HTTPS vulnérable 6
    3.5. Déchiffrement d'interceptions anciennes 6
    3.6. Déchiffrement d'interceptions récentes 7
    3.7. Imitation de sites sécurisés 7
    3.8. Extraction de données depuis un navigateur HTTPS vulnérable, par phishing 8
    3.9. Extraction de données depuis un navigateur HTTPS vulnérable, via des liens tiers 9
    3.10. Extraction de données depuis un aspirateur d'URLs vulnérable 9
    3.11. Analyse et corrélation de trafic Tor 10
    3.12. Identification de serveurs cachés et d'utilisateurs par des noeuds Tor hostiles 11
    3.13. Attaques contre les services VPN 11
    3.14. Attaques contre les proxys HTTPS vulnérables 12
4. Perspectives 12
5. Impact prévisible à long terme 13
6. Remerciements 13
Bibliographie 13

1. Contexte

La faille "Heartbleed" est vraisemblablement la pire chose qui soit arrivée à la sécurité sur Internet. À cause d'elle, HTTPS est moins sûr que HTTP, car les pirates peuvent obtenir des données confidentielles sans avoir besoin d'intercepter les échanges. Pour les détails techniques sur le bug lui-même, voir [HEARTBLEED], [CVE-2014-0160] et [XKCD1354].

Les premières réactions se sont focalisées sur la mise à jour des serveurs web vulnérables, la révocation des certificats SSL et le renouvellement des mots de passe. Il a fallu quelques jours de plus pour comprendre que la faille Heartbleed affecte également les logiciels clients, les échanges SSL autres que HTTPS, et une multitude d'appareils embarqués qui ne recevront jamais de mise à jour logicielle.

2. Notations

Dans la suite de ce document divers scénarios d'attaque sont illustrés par des *Message Sequence Charts*. Des exemples de code source LaTeX sont disponibles (Section 6, « Remerciements »).

Conformément à l'usage dans les publications de cryptographie, des prénoms conventionnels identifient les rôles des participants :

- **Alice**, **Bob** : Des utilisateurs de services en ligne sécurisés.
- **Eve** : Un attaquant passif qui espionne les échanges.
- **Trudy** : Un attaquant actif qui peut exploiter la faille Heartbleed en envoyant des messages *heartbeat* anormaux sur une connexion SSL (par exemple HTTPS).
- **yuri.com** : Un site web dont l'implémentation de SSL contient la faille Heartbleed.

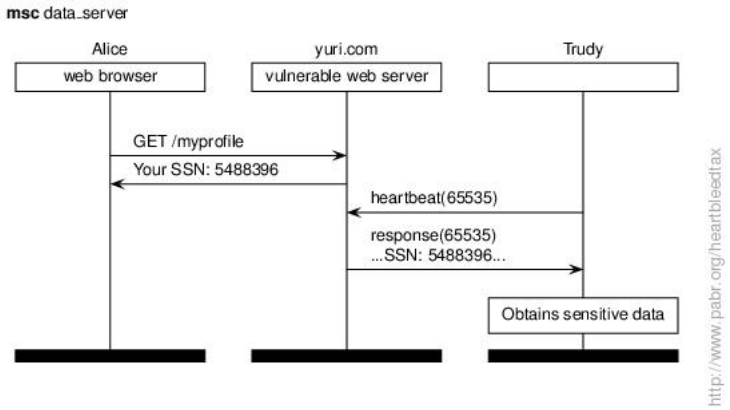
  Comme OpenSSL est très utilisé sur Internet, il faut considérer que n'importe quel site web peut jouer le rôle de yuri.com jusqu'à preuve du contraire.
- **george.com** : Un site web dont l'implémentation de SSL n'est pas ou plus concernée par Heartbleed.

  Tous les grands sites Internet sont maintenant dans cette situation, mais il est probable que des milliers de petits sites ne communiqueront jamais sur leur gestion de l'affaire Heartbleed, laissant leurs utilisateurs dans le doute. Pour évaluer la situation de votre site préféré, commencez par interroger [LASTPASS]. Vous pouvez également vérifier manuellement que son certificat a une date *NotBefore* postérieure au 7 avril 2014. Cela suggère que le site a fait le nécessaire (mais des faux positifs et des faux négatifs sont possible car un site peut renouveler un certificat expiré sans changer les clés, et aussi changer les clés dans modifier les dates de validité). En dernier recours, [FILIPPO] permet de tester si un site est toujours vulnérable. Avertissement : Ce service va "attaquer" le serveur à votre demande, ce qui peut vous exposer à des poursuites en justice.
- **Victor** : Un utilisateur dont les logiciels clients SSL comportent la faille Heartbleed.

  Pour déterminer si vous êtes dans la situation de Victor plutôt que d'Alice, vérifiez la version de vos packages OpenSSL et/ou libSSL. Les version 1.0.1 à 1.0.1f sont vulnérables (sauf si compilées avec des options particulières). D'après [ARS_CLIENTS], Android 4.1.1 est concerné. En cas de doute, voyez [REVERSEHEARTBLEED]. Avertissement : Ne diffusez par les URL malicieuses générées par ce service.
- **mallory.com** : Un serveur hostile qui peut se faire passer pour un autre site web ou attaquer les clients SSL vulnérables.
- **brad.com** : Un prestataire qui héberge du contenu pour d'autres sites web, par exemple des bandeaux publicitaires, des ressources statiques, des compteurs d'accès, des bibliothèques Javascript, des feuilles de style CSS, des fichiers multimédia.

3. Scénarios d'attaques et contre-mesures

3.1. Extraction de données sensible depuis un serveur HTTPS vulnérable



Dans ce scénario **Alice** saisit ou consulte des données sensibles sur **yuri.com**. Les données déchiffrées restent dans la mémoire du serveur web tant que les buffers ne sont pas réutilisés. Peu après, **Trudy** se connecte comme un client HTTPS ordinaire et récupère ces données en exploitant la faille Heartbleed.

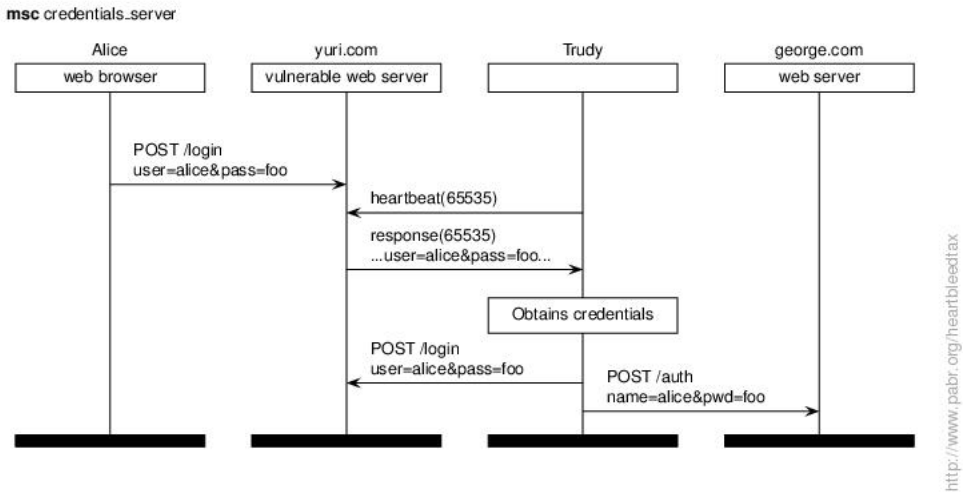
Contre-mesures pour les utilisateurs.

- Évitez d'échanger des données sensibles avec un site web jusqu'à ce qu'il ait traité le problème Heartbleed.

Sources.

- *Canadian charged in 'Heartbleed' attack on tax agency* [http://www.reuters.com/article/2014/04/16/us-cybersecurity-heartbleed-arrest-idUSBREA3F1KS20140416] (reuters.com)

3.2. Extraction de données d'authentification depuis un serveur HTTPS vulnérable



Dans ce scénario **Alice** s'authentifie auprès de **yuri.com** en fournissant un login et un mot de passe sur HTTPS. Peu après, **Trudy** se connecte comme un client HTTPS ordinaire et récupère ces informations

en exploitant la faille Heartbleed. **Trudy** peut alors accéder aux comptes d'**Alice** sur **yuri.com** et sur tout autre site où elle a utilisé les mêmes identifiants.

Contre-mesures pour les utilisateurs.

- Évitez de saisir vos identifiants sur un site web jusqu'à ce qu'il ait traité le problème Heartbleed.
- Ensuite, changez vos mots de passe.
- Dans l'intervalle, méfiez-vous des tentatives de *phishing*, par exemple des emails vous invitant à venir changer vos mots de passe sur un faux site web.

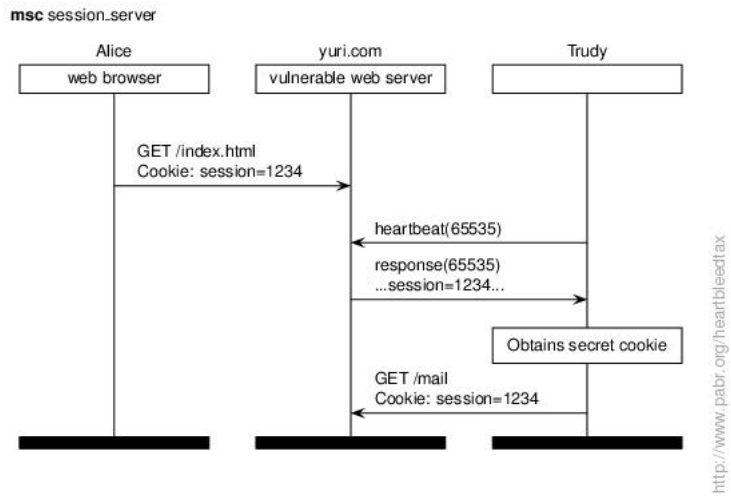
Leçons.

- Ne jamais utiliser un même mot de passe sur plusieurs sites.
- Utiliser des procédures d'authentification à plusieurs facteurs.
- Utiliser l'authentification mutuelle SSL (certificats clients) ?

Sources.

- *"The passwords and personal messages of up to 1.5 million Mumsnet users may have been exposed"* [http://www.telegraph.co.uk/technology/internet-security/10766872/Heartbleed-hackers-hit-Mumsnet-website.html] (telegraph.co.uk)

3.3. Détournement de session sur un serveur HTTPS vulnérable

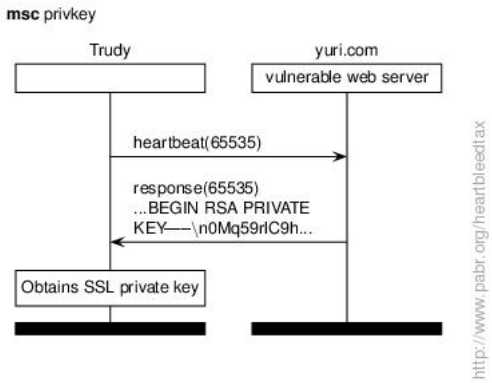


Dans ce scénario **Trudy** extrait un cookie de session plutôt que des données d'authentification. Ceci lui permet de prendre le contrôle du compte d'**Alice** sans attendre qu'elle saisisse ses identifiants.

Contre-mesures pour les utilisateurs.

- Déconnectez-vous de vos services en ligne jusqu'à ce qu'ils aient traité le problème Heartbleed.

3.4. Extraction de la clé privée SSL d'un serveur HTTPS vulnérable



Dans ce scénario **Trudy** extrait la clé privée SSL/TLS de **yuri.com**. Quel que soit l'usage qu'elle en fera ensuite (voir les sections suivantes), la perte d'une clé privée est en soi une catastrophe.

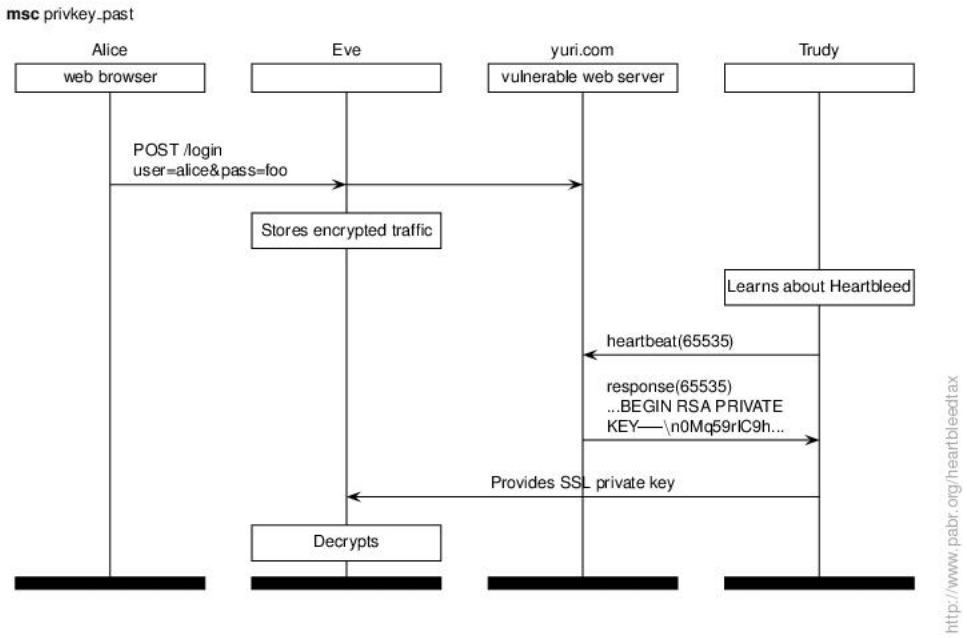
Leçons.

- Protéger les clés privées dans un module matériel de sécurité (*hardware security module*).

Sources.

- *Confirmed: Heartbleed Exposes Web Server's Private SSL Keys* [http://www.securityweek.com/confirmed-heartbleed-exposes-web-servers-private-ssl-keys] (securityweek.com)

3.5. Déchiffrement d'interceptions anciennes



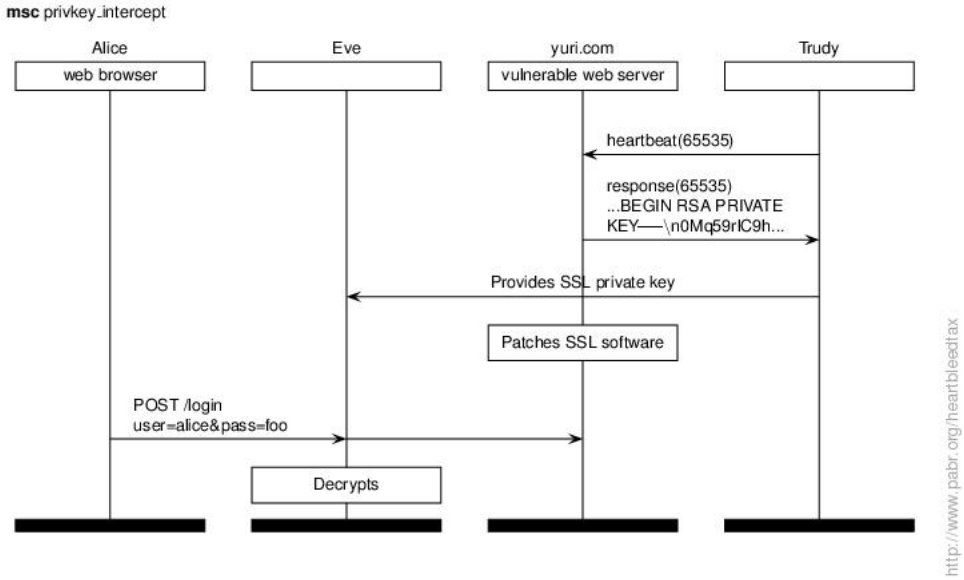
Dans ce scénario **Trudy** extrait la clé privée SSL de **yuri.com** et l'utilise pour déchiffrer des échanges espionnés par **Eve** longtemps auparavant, y compris avant l'introduction de la faille Heartbleed dans OpenSSL.

C'est le jackpot pour les organisations qui s'amusent à archiver des petaoctets de données chiffrées !

Leçons.

- Utiliser des protocoles cryptographiques à confidentialité persistante.
- Renouveler les paires de clés régulièrement.

3.6. Déchiffrement d'interceptions récentes

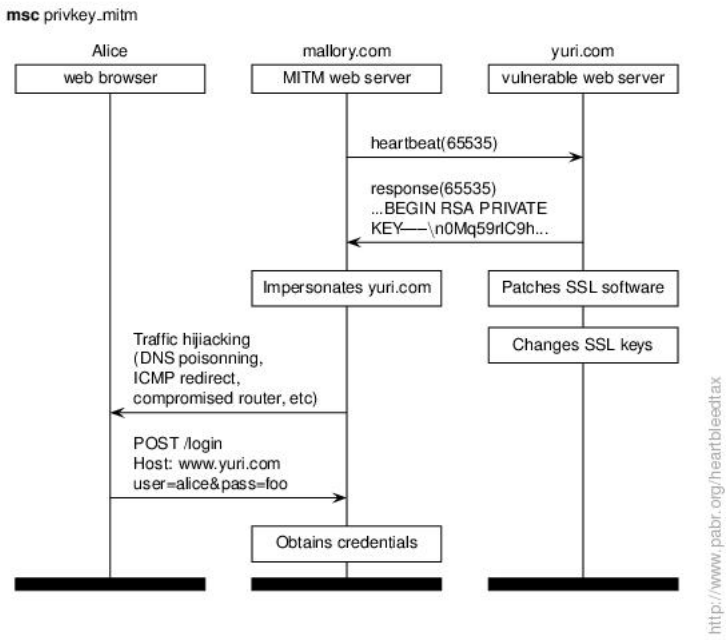


Dans ce scénario **Trudy** extrait la clé privée SSL de **yuri.com** et l'utilise pour déchiffrer des échanges interceptés, y compris après que **yuri.com** ait mis à jour son implémentation de SSL.

Contre-mesures pour les utilisateurs.

- Vérifiez que les sites concernés ont soit changé leurs clés, soit annoncé que les clés n'ont pas été compromises.

3.7. Imitation de sites sécurisés



Ici **mallory.com** se fait passer pour **yuri.com** après avoir extrait sa clé privée SSL. Ce scénario appelé "attaque de l'homme du milieu" (man-in-the-middle attack) est plus dangereux que l'espionnage passif, car **mallory.com** peut forcer **Alice** à utiliser un certificat compromis. **mallory.com** peut également contourner certaines procédures de sécurité multi-facteurs.

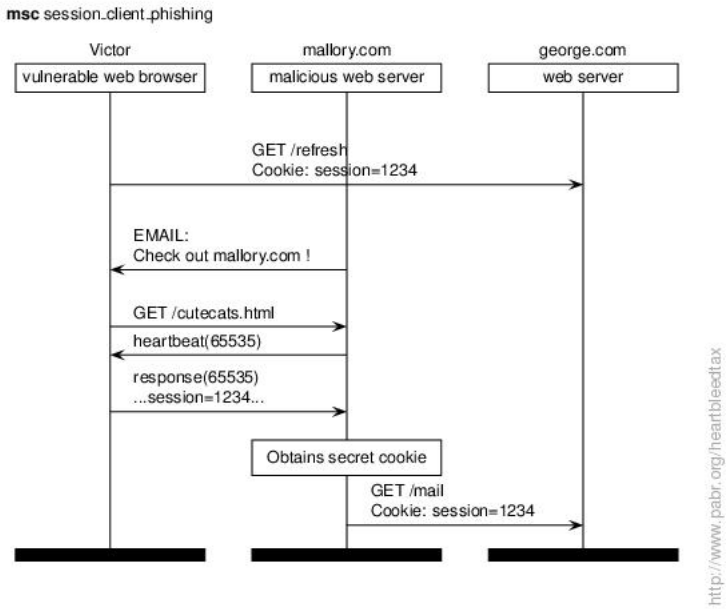
Contre-mesures pour les utilisateurs.

- Vérifiez si votre navigateur détecte les certificats révoqués : [REVOKED_GRC].
- À défaut, inspectez les certificats manuellement.

Leçons.

- Heartbleed a révélé les faiblesses de l'infrastructure actuelle de gestion des certificats révoqués. [LANGLEY] explique le problème et mentionne des solutions telles que OCSP stapling et DNSSEC.

3.8. Extraction de données depuis un navigateur HTTPS vulnérable, par phishing

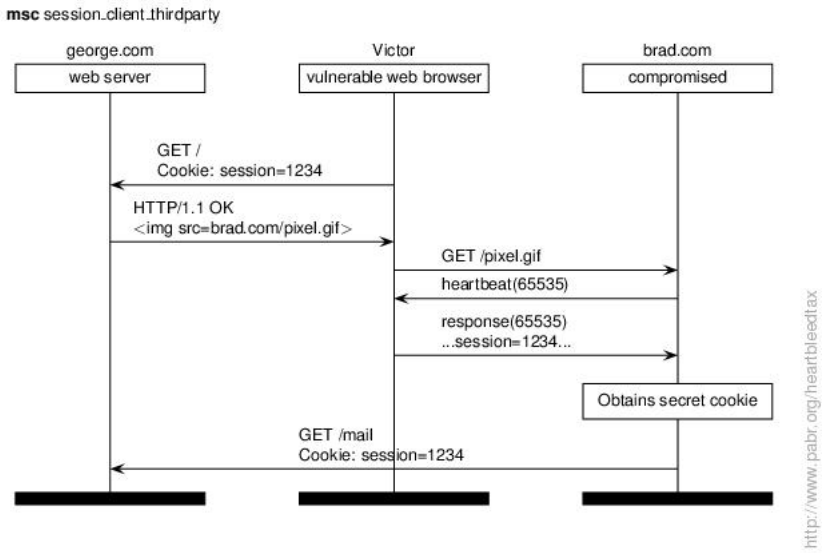


Dans ce scénario **mallory.com** extrait des données de **Victor** dont le logiciel client SSL est vulnérable.

Contre-mesures pour les utilisateurs.

- Mettez vos logiciels à jour.
- Utilisez des comptes d'utilisateurs distincts ou des instances de navigateurs séparées pour le surf anonyme et pour les transactions sensibles.

3.9. Extraction de données depuis un navigateur HTTPS vulnérable, via des liens tiers

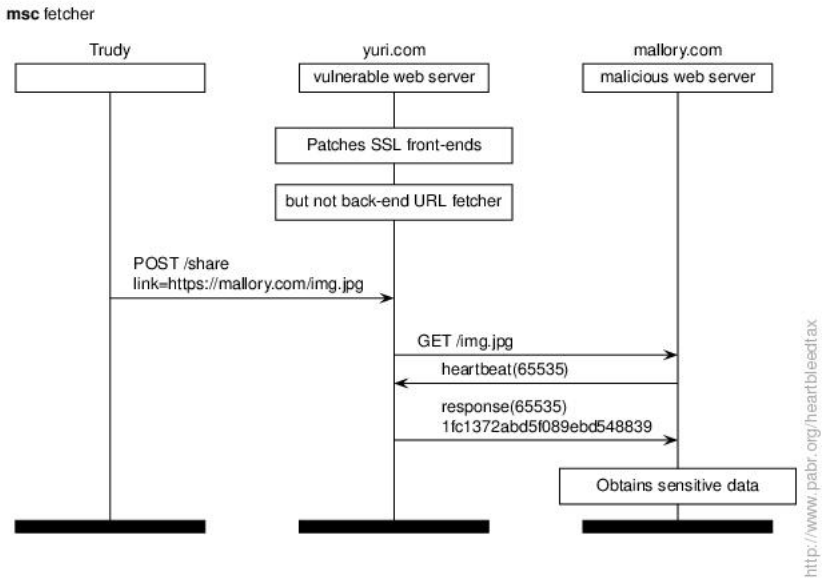


Dans ce scénario **Trudy** prend le contrôle de **brad.com**, un prestataire parmi d'autres qui fournit du contenu référencé dans les pages de **george.com**. **Victor** se fait attaquer alors qu'il pensait communiquer uniquement avec **george.com**, à qui il fait confiance.

Contre-mesures pour les utilisateurs.

- Mettez vos logiciels à jour.
- Filtrez les contenus tiers.

3.10. Extraction de données depuis un aspirateur d'URLs vulnérable



Ici **Trudy** incite **yuri.com** à télécharger un document depuis **mallory.com**, qui en profite pour extraire des données du back-end vulnérable de **yuri.com**. Ce scénario concerne les robots d'indexation des moteurs de recherche, les réseaux sociaux qui examinent les liens partagés par leurs utilisateur, les services de traduction de pages web, les testeur de conformité HTML, etc. Cependant il n'est pas certain que des données réellement sensibles puissent être perdues de cette façon.

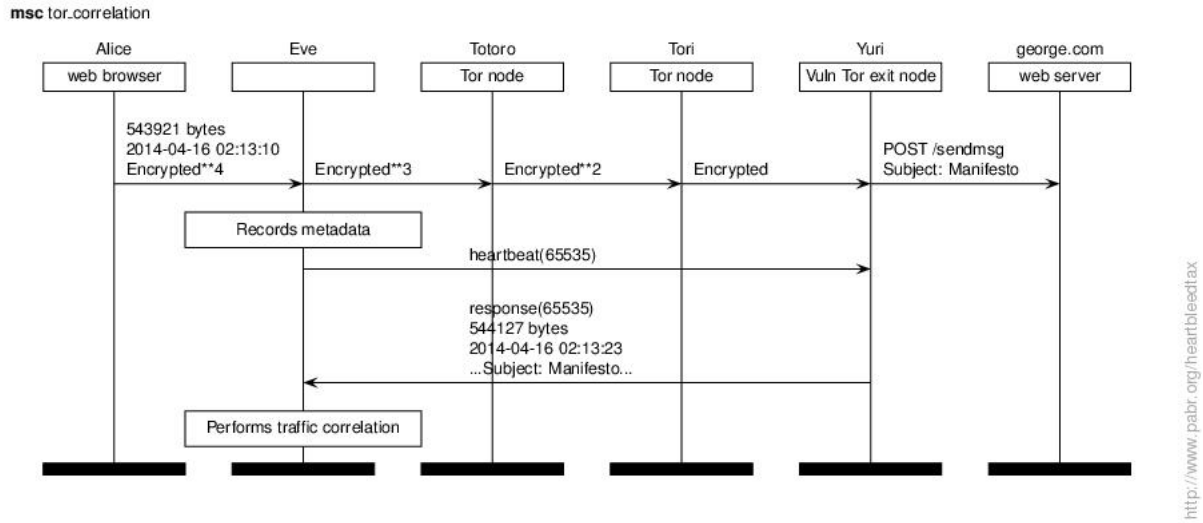
Leçons.

- Il faut administrer les machines de back-end aussi soigneusement que les front-ends web.

Sources.

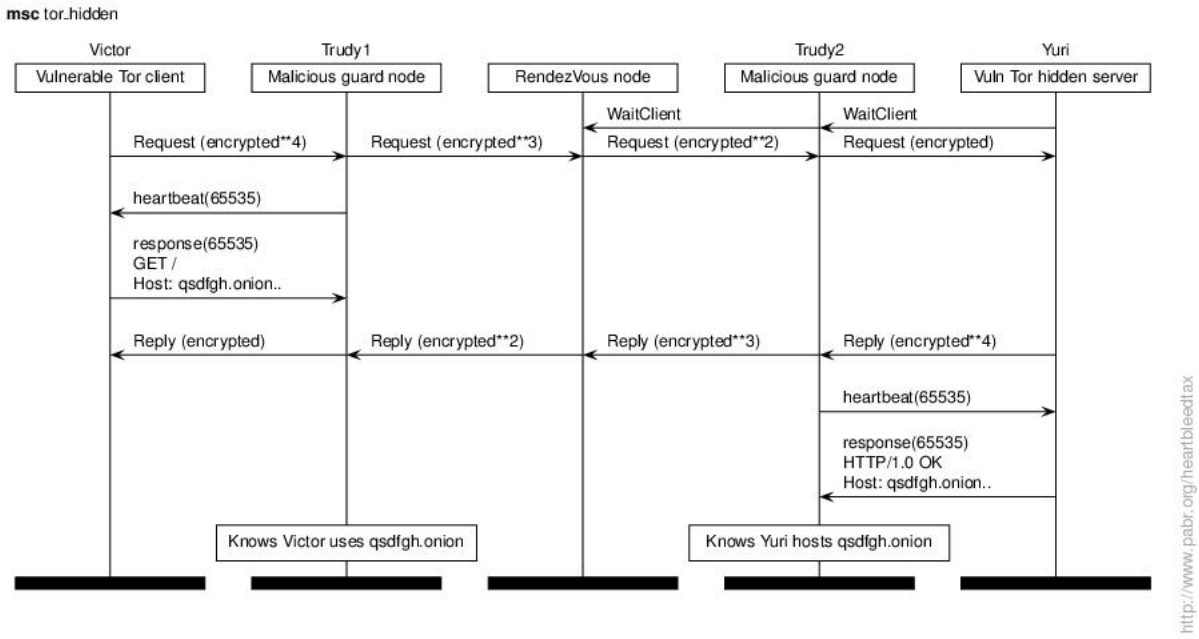
- *Testing for "reverse" Heartbleed - What did we find ?* [http://blog.meldium.com/home/2014/4/10/testing-for-reverse-heartbleed] (meldium.com)

3.11. Analyse et corrélation de trafic Tor



Eve, à la tête d'une dictature, veut prouver que **Alice** utilise Tor pour communiquer avec **george.com**, une organisation humanitaire étrangère. **Eve** peut espionner tout le trafic Internet sur son territoire mais n'a aucun pouvoir à l'étranger. Elle exploite massivement la faille Heartbleed contre les noeuds de sortie Tor vulnérables afin de corréler le trafic sortant avec ses interceptions locale.

3.12. Identification de serveurs cachés et d'utilisateurs par des noeuds Tor hostiles

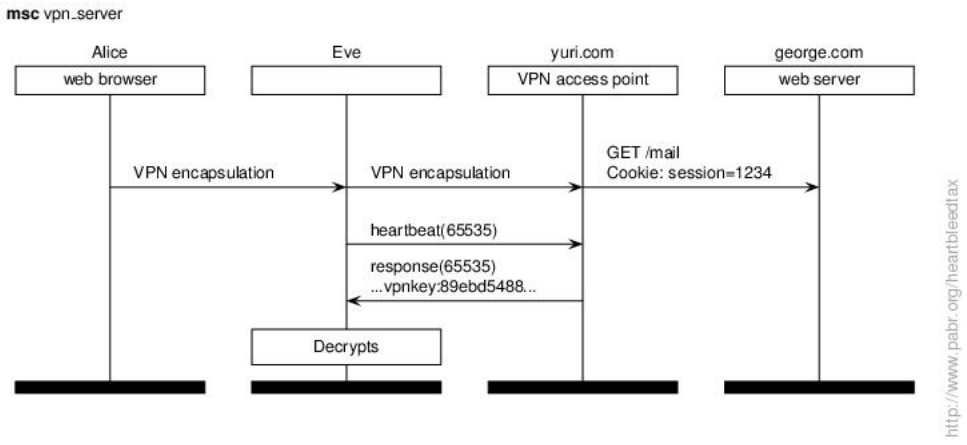


Trudy déploie un grand nombre de noeuds d'entrée Tor piégés. Elle exploite la faille Heartbleed contre les clients qui s'y connectent, y compris les serveurs Tor cachés et leurs utilisateurs. Bien que les services cachés Tor soient chiffrés de bout en bout, **Trudy** peut identifier leurs utilisateurs et hébergeurs vulnérables en examinant les échanges en clair révélés par Heartbleed. De plus, si elle extrait la clé privée d'un service caché, elle peut se faire passer pour ce service.

Sources.

- *"Tor hidden services might leak their long-term hidden service identity keys to their guard relays."* [https://blog.torproject.org/blog/openssl-bug-cve-2014-0160] (torproject.org)

3.13. Attaques contre les services VPN



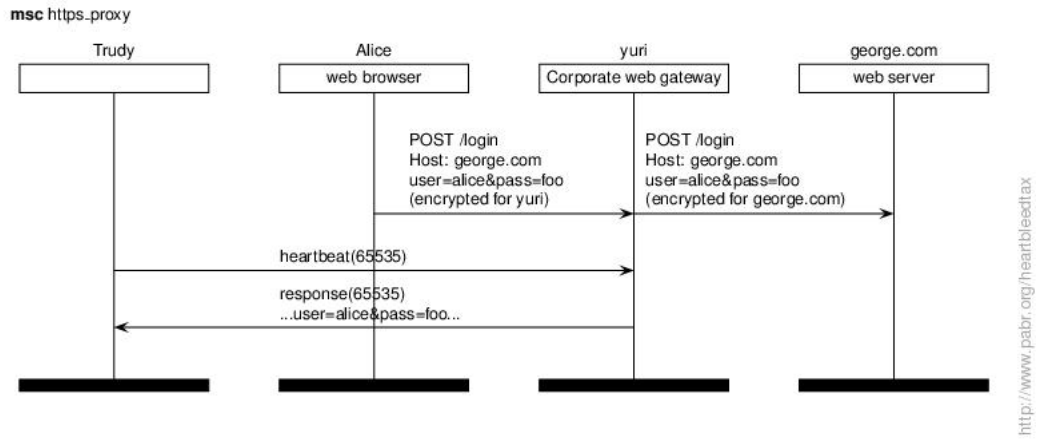
Alice est consciente que les réseaux WiFi publics n'offrent généralement aucune confidentialité. Elle a donc configuré son smartphone et son ordinateur portable pour accéder à Internet via un service de VPN, **yuri.com**. (Alternativement, elle pourrait faire tourner un serveur VPN chez elle, ou utiliser la fonction VPN de sa "box" ADSL ou de son serveur NAS.) **Eve** espionne le réseau WiFi sur lequel **Alice**

est connectée, remarque un trafic VPN sur SSL en provenance de son smartphone, exploite Heartbleed contre l'adresse IP destinataire, et extrait soit la clé du VPN, soit les échanges en clair.

Sources.

- *Attackers Exploit the Heartbleed OpenSSL Vulnerability to Circumvent Multi-factor Authentication on VPNs* [https://www.mandiant.com/blog/attackers-exploit-heartbleed-openssl-vulnerability-circumvent-multifactor-authentication-vpns/] (mandiant.com)
- *"OpenVPN uses OpenSSL as its crypto library by default and thus is affected"* [http://community.openvpn.net/openvpn/wiki/heartbleed] (openvpn.net)

3.14. Attaques contre les proxys HTTPS vulnérables



Alice consulte son compte bancaire depuis son poste de travail. Elle a vérifié que le site de sa banque, **george.com**, n'est pas touché par Heartbleed. Cependant, son employeur route le trafic web sortant via **yuri**, un proxy chargé de détecter les virus et les usages abusifs. Pour inspecter les échanges HTTPS, **yuri** joue le rôle d'une autorité de certification reconnue par le navigateur d'**Alice** (il va générer un certificat à la volée pour **george.com**). **Trudy**, une collègue d'**Alice**, exploite Heartbleed contre le proxy et extrait des informations sensibles.

Contre-mesures pour les utilisateurs.

- Évitez d'échanger des données sensibles avec un site web jusqu'à ce que votre administrateur réseau ait traité le problème Heartbleed.

Leçons.

- Le maillon faible de la chaîne de confiance n'est pas toujours où l'on croit.

Sources.

- Liste de passerelles web et autres équipements de sécurité concernés par Heartbleed [https://www.cert.fi/en/reports/2014/vulnerability788210.html] (cert.fi)

4. Perspectives

Au delà de HTTPS, de nombreux services et protocoles basés sur SSL/TLS pourraient s'avérer touchés par la faille Heartbleed :

- des tiers de confiance d'horodatage ou de notarisation, où les clés privées sont utilisées à des fins de signature plutôt que de chiffrement ;
- des systèmes de téléchargement automatique de mises à jour de logiciels ;

- RADIUS, Diameter et d'autres protocoles de sécurité similaires, lorsqu'ils sont utilisés sur TLS ;
- SMTPS, POP3S, IMAPS ;
- SIPS ;
- des systèmes de monnaie électronique et des applications de porte-monnaie ;
- des infrastructures de développement open-source (git) ;
- des systèmes de vote électronique.

5. Impact prévisible à long terme

On peut espérer que l'affaire Heartbleed servira à sensibiliser les utilisateurs à la sécurité sur Internet et conduira à des progrès, notamment :

- La promotion de langages de programmation à la fois sûrs et efficaces.
- Une modernisation de l'infrastructure de certification X509 afin que les logiciels clients n'aient plus d'excuse pour ne pas détecter les certificats révoqués.

6. Remerciements

Les MSC sont dessinés à l'aide de [MSCSTY]. Voici un exemple de code source LaTeX : credentials_server.tex

Bibliographie

[HEARTBLEED] *The Heartbleed Bug* . http://heartbleed.com.

[CVE-2014-0160] *CVE-2014-0160*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160.

[XKCD1354] *How the Heartbleed bug works* . Randall Munroe. http://xkcd.com/1354/.

[FILIPPO] *Heartbleed Test* . https://filippo.io/Heartbleed/.

[LASTPASS] *LastPass Heartbleed checker* . https://lastpass.com/heartbleed/.

[REVOKED_GRC] *Security Certificate Revocation Awareness Test* . https://revoked.grc.com/.

[ARS_CLIENTS] *Vicious Heartbleed bug bites millions of Android phones, other devices* . http://arstechnica.com/security/2014/04/vicious-heartbleed-bug-bites-millions-of-android-phones-other-devices/.

[REVERSEHEARTBLEED] *Reverse Heartbleed Tester* . https://reverseheartbleed.com/.

[LANGLEY] *No, don't enable revocation checking* . Adam Langley. https://www.imperialviolet.org/2014/04/19/revchecking.html.

[MSCSTY] *Drawing Message Sequence Charts with LaTeX* . Sjouke Mauw et Victor Bos. http://satoss.uni.lu/software/mscpackage/.