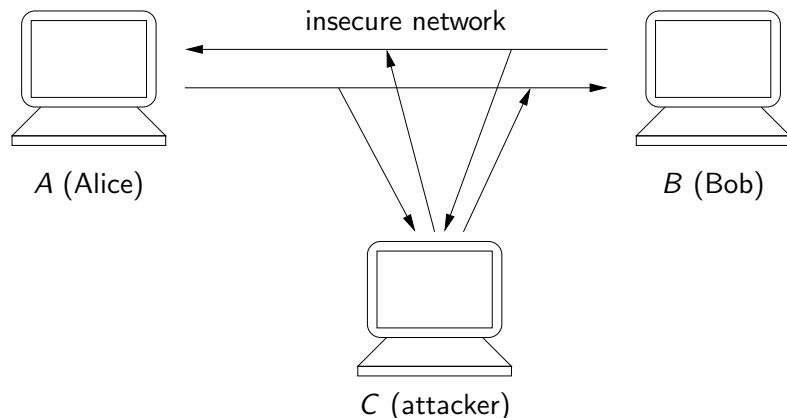


Protocoles cryptographiques: Attaques – Vérification

Bruno Blanchet

INRIA Paris-Rocquencourt
Bruno.Blanchet@inria.fr

Juin 2014



Un attaquant peut

- écouter les messages
- envoyer ses propres messages

- Utiliser la cryptographie pour sécuriser les communications
- Par exemple, chiffrer les données pour préserver le secret

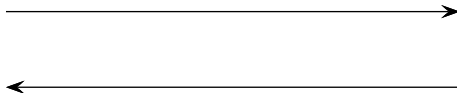
Chiffrement symétrique



Les protocoles cryptographiques sont partout



Employé nomade

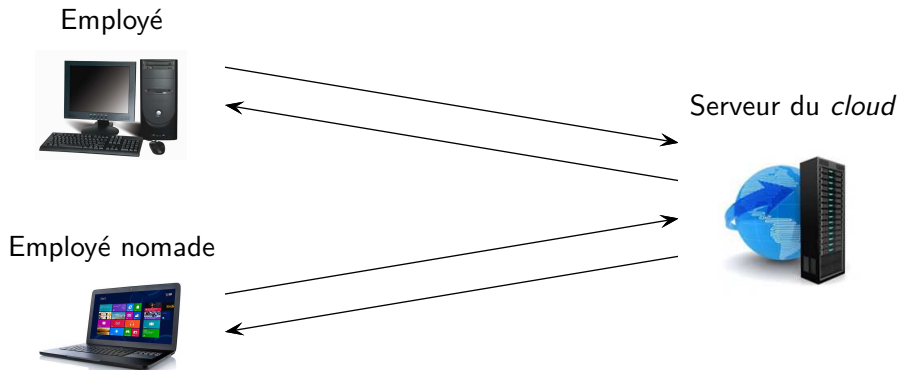


Serveur d'entreprise



Protocoles habituels : TLS (`https://`) ou IPsec (VPN)

Stockage sur le *cloud*



On fait confiance au fournisseur du *cloud* pour :

- ne pas regarder les données de ses clients ;
- protéger les clients les uns des autres.

Sinon, il faut chiffrer les données avant de les envoyer au *cloud*.

- Des erreurs peuvent apparaître à différents niveaux :
 - primitives
 - protocole
 - implémentation
- Les erreurs de sécurité apparaissant seulement en présence d'un attaquant.
 - Elles ne sont pas détectées par les tests.

⇒ Beaucoup d'attaques sont découvertes contre des protocoles cryptographiques.

Une attaque récente et grave

Faible Heartbleed : les sites pour lesquels il est conseillé de changer son mot de passe

Le Monde.fr | 11.04.2014 à 04h48 • Mis à jour le 14.04.2014 à 15h08 |

Par Michael Szadkowski

Abonnez-vous à partir de 1 €

Réagir

Classer

Partager

Partager

Recommander Partager 14 010 personnes le recommandent.



Deux jours après la révélation d'une faille de sécurité au sein du protocole OpenSSL, baptisée « Heartbleed », cette dernière est décrite par certains comme « le pire cauchemar » qui puisse arriver concernant la sécurité des échanges sur Internet.



Le logiciel libre OpenSSL est installé sur les serveurs de très nombreux sites pour établir des connexions chiffrées et sécurisées entre ce dernier et ses utilisateurs. De très nombreux sites Internet utilisent OpenSSL pour sécuriser leurs échanges.

Faill...

Faill...

lesquel...

son mo...

Le Monde.fr | 11.04

Par Michael Szad

Abonnez-vous à partir de 1€

Recommander



000101010100
101010010101
101001010100
101001010010
100101010100
00101010100
101010101000
101010010100
010101001010
010100100101

Le changement annoncé avoir affecte le proto

Deux jours après OpenSSL, baptisé « le pire cauchemar Internet.



Le logiciel libre C établir des connexions De très nombreux

tech-medias • actu

Lesechos.fr • Le 24 avril 2014

Faill...

» : les leçons à tirer

La faille informatique baptisée Heartbleed est maintenant réparée. Mais les entreprises ont beaucoup à apprendre de ce malheureux épisode. La confidentialité des données de leurs clients a été mise en danger.



L'hémorragie est arrêtée. Entre mars 2012 et le 7 avril 2014, la faille informatique Heartbleed (« cœur qui saigne », en anglais) a concerné un très grand nombre de sites Internet, des réseaux sociaux en passant par les banques

en ligne et les plates-formes de e-commerce. Le comble est que le danger provient justement du système chargé de sécuriser l'accès aux services sensibles comme le paiement en ligne...

L'alerte n'intervient que dans les premiers jours d'avril 2014. Jusqu'ici personne n'avait constaté de péril. Le risque : des cyber-criminels pouvaient facilement retrouver les informations personnelles d'internautes utilisateurs de ces sites, dans la mémoire des serveurs informatiques. Noms et mots de passe en premier lieu. Quelques jours après la

Une attaque récente et grave

M TechLesEcho

TECHNOLOGIES

Jeux vidéo

FRANCE

INTERNATIONAL

Faible H lesquel son mo

Le Monde.fr | 11.04

Par Michael Szad

Abonnez-vous
à partir de 1 €

Recommander

000101010100
101010010101
101001010100
101001010010
100101010100
000101010000
101010101000
101010010100
010101001010
010100100101

Le changement
annoncé avoir
affecte le proto

Deux jours après
OpenSSL, baptis
« le pire cauche
Internet.



Le logiciel libre C
établir des conne
De très nombreu

tech-medias • a
Lesechos.fr • Le

Faible : » : les l

La faille infi
réparée. Ma
malheureux
clients a été



en ligne et les
justement du sys
paiement en lign

L'alerte n'inten
n'avaient constat
les informations |
serveurs informa



L'IMPACT DE LA FAILLE HEARTBLEED S'ÉTEND BIEN AU-DELÀ D'INTERNET

Recommander 6 8+1 0

11/04/14



par Jim Finkle

BOSTON (Reuters) - La faille de sécurité "Heartbleed" pourrait permettre à des pirates informatiques d'accéder à des boîtes mail, de contourner des pare-feu, voire de pirater des téléphones portables, selon des spécialistes en informatique qui ont prévenu jeudi que les risques pourraient s'étendre au-delà des seuls serveurs internet.

Une attaque récente et grave

Faill...

lesquel

son mo

Le Monde.fr | 11.04

Par Michael Szad

Abonnez-vous à partir de 1 €

Recommander

000101010100
101010010101
101001010100
101001010010
100101010100
100101010100
101010101000
101010010100
101010010101
010100100101

Le changement annoncé avoir affecte le proto

Deux jours après OpenSSL, baptisé « le pire caucher Internet.

Le logiciel libre C établir des conn De très nombre

tech-medias • a

Lesechos.fr • Le

Faill :

» : les l

La faille info réparée. Ma malheureux clients a été



en ligne et les justement du sys paiement en lign

L'alerte n'inter n'avaient constat les informations | serveurs informa

The Heartbleed Hit List: The Passwords You Need to Change Right Now

661.6k

Share on Facebook

Share on Twitter



L'I

HE

BI

D'I

Recom



par Jim

BOSTO!
informa
des télé
que les r



It's time to update your passwords to various sites affected by the Heartbleed bug.

IMAGE: MASHABLE COMPOSITE. (ISTOCKPHOTO, ZORBER)

Une attaque récente et grave

M TechLesEcho

TECHNOLOGIES Jeux vidéo FRANCE + INTERNATIONAL

Faill...

Le Monde.fr | 11.04
Par Michael Szad

Abonnez-vous à partir de 1 €

Recommander

00101010100
10101001010
10100101010
10100101010
10100101010
10010101010
10010101010
10101010100
10101001010
10101001010
10101001010
10100100101

Le changement annoncé avoir affecte le proto

Deux jours après OpenSSL, baptis « le pire caucher Internet.

Le logiciel libre C établir des conne De très nombre

tech-medias + a

Lesechos.fr • Le

Faill...

» : les l
La faille infé réparée. Ma malheureux clients a été

en ligne et les justement du sys paiement en ligne

L'alerte n'inten n'avaient constat les informations | serveurs informa

Mashable

The Heartbleed Password Right M

661.6k

L'HEBI D'I

Recom

f

par Jim

BOSTON informa des télé que les r

The Register

Data Centre Software Networks Security Policy Business Hardware Science Bootnotes Columnists

SECURITY

Anatomy of OpenSSL's Heartbleed: Just four bytes trigger horror bug

The code behind the C-bomb dropped on the world

By Chris Williams, 9 Apr 2014 [Follow](#) 1,190 followers

145

RELATED STORIES

Get cracking on STARTTLS says Facebook

Apple splats 'new' SSL snooping bug in iOS, OS X - but it's no Heartbleed

OpenBSD founder wants to bin buggy OpenSSL library, launches fork

Fixing OpenSSL's Heartbleed flaw will take MONTHS, warns Secunia

Analysis The password-leaking OpenSSL bug dubbed Heartbleed is so bad, switching off the internet for a while sounds like a good plan.

A tiny flaw in the widely used encryption library allows anyone to trivially and secretly dip into vulnerable systems, from your bank's HTTPS server to your private VPN, to steal passwords, login cookies, private crypto-keys and much more.

How, in 2014, is this possible?

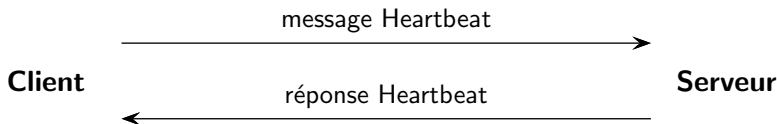
A simple script for the exploit engine Metasploit can, in a matter of seconds, extract sensitive in-memory data from systems that rely on OpenSSL 1.0.1 to 1.0.1f for TLS encryption. The bug affects about 500,000, or 17.5 per cent, of trusted HTTPS websites, we're told, as well as client software, email servers, chat services, and anything else using the aforementioned versions of OpenSSL.

A good number of popular web services have now been patched following disclosure of the vulnerability on Monday; you can use this tool to check (use at your own risk, of course), but don't forget to do more than patch your OpenSSL installation if you're affected - change your keys, dump your session cookies and evaluate your at-risk data.

Too long, didn't read: A summary

Heartbleed expliqué

- SSL/TLS : protocole utilisé pour les pages web `https://`.
- Heartbeat : une extension de TLS qui vérifie juste qu'un serveur est vivant.
 - Le client envoie un packet au serveur.
 - Le serveur répond au client avec le même paquet.



- L'attaque :
 - 1 Un client malhonnête envoie un octet mais dit qu'il a envoyé 65535 octets.
 - 2 Le serveur répond avec 65535 octets : l'octet du client et les 65534 octets suivants de sa mémoire.

Pour détecter ces attaques, il faut **vérifier les protocoles formellement**.

Plusieurs niveaux :

- Primitives cryptographiques
- Spécification du protocole : description formelle du protocole
- Implémentation : le programme qui implémente le protocole
- Niveau physique : carte à puce, ...

	Modèle symbolique	Modèle calculatoire
Messages	Termes $\text{encrypt}(M, K)$	Chaînes de bits 0100011
Primitives	Symboles de fonction encrypt	Fonctions sur les chaînes de bits
Attaquant	Restreint à n'utiliser que les primitives	N'importe quel algorithme

- Penser tôt à la sécurité
 - Quand il y a une attaque, il est trop tard !
- Utiliser les outils disponibles, ne pas chercher à recréer ses propres protocoles
- Faire des mises à jour régulières
- Les méthodes formelles peuvent servir
 - miTLS, une implémentation de référence vérifiée de TLS,
www.mitls.org