- poodle

-BERserk

-Heartbleed

## -Triple Handshake attack -<http://www.darkreading.com/vulnerabilities---threats/new-openssl-flaw-exposes-ssl-to-man-in-the-middle-attack/d/d-id/1269452> : CVE-2014-0224 (mini attaque MIT)

- <http://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack>:

([CVE-2014-3511](https://www.openssl.org/news/secadv_20140806.txt)) permet d’utiliser une version anterieur de ssl pour utiliser une faille

- cookie cutter attack https://secure-resumption.com/tlsauth.pdf

- virtual host confusion https://hackerone.com/reports/501

**Triple Hanshake Attack :**

Source :

* [https://secure-resumption.com](https://secure-resumption.com/)
* [/](https://secure-resumption.com/)<http://blog.cryptographyengineering.com/2014/04/attack-of-week-triple-handshakes-3shake.html>

le premier lien est écrit par des chercheurs de l’INRIA de paris-Rocquencourt (très fiable)

c’est eux qui ont présenté l’attaque (je crois) l’article date de mai 2014

Attaque basé sur la partie “handshake” du potocole (c’est à dire l’accord pour la clé )

Protocole en 3 passe pour que le serveur et le client choisisse une clé de session

le protocole de Diffie-Hellman par exemple

Man in the middle (evidement) pour intercepté les clés.

Cette attaque n’est pas une faille au sens crypto mais au niveau de l’implementation TLS.

probleme sur les certificats

#### **Hearthbleed**

#### 

#### CVE-2014-0160

http://en.wikipedia.org/wiki/Heartbleed

Overflow : envoie d’une requête Heathbleed message : un payload suivi de la taille du payload (16 bit) la réponse a exactement le même payload.

Problème : on peut envoyer un message court mais avec une taille de payload très grande.

Quand le serveur va vouloir renvoyer, il va recopier le payload soit taille du payload élément.

Le payload etant plus petit, il va lire en dehors du buffer

Aucun controle sur les données qui vont être ecrite en plus