

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

# Heartbleed, Technical Overview

Bruno Pujos

May 13, 2014

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

## 1 Introduction

## Introduction

- The Open Source toolkit for SSL/TLS
- Begin in 1998
- SSL/TLS
- Heartbeat - CVE-2014-0160
  - Heartbeat extension (RFC6520)
  - Release on 14/03/12 (OpenSSL 1.0.1)
  - Patch on 07/04/14 (OpenSSL 1.0.1g)

Heartbleed

Memory Leak

Conclusion

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

## 2 Heartbleed

*A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64k of memory to a connected client or server.*

*Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including 1.0.1f and 1.0.2-beta1.*

*Thanks for Neel Mehta of Google Security for discovering this bug and to Adam Langley <agl@chromium.org> and Bodo Moeller <bmoeller@acm.org> for preparing the fix.*

- Heartbeat Extension (RFC6520)
- for TLS and DTLS (Datagram Transport Layer Security)
- design to do PMTUD (path maximum transmission unit discovery)
- 2 message types:
  - HeartbeatRequest
  - HeartbeatResponse
- Work in both way (with client attacking and with server attacking)

# HeartbeatMessage structure

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

```
struct {
    HeartbeatMessageType type;
    uint16 payload_length;
    opaque payload[payload_length];
    opaque padding[padding_length];
} HeartbeatMessage;
```

## HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "POTATO" (6 LETTERS).



Secure connection using key "4538538374224"  
User Meg wants these 6 letters: POTATO. User  
ida wants pages about "irl games". Unlocking  
secure records with master key 5130985733435  
Alice (browser) sends this message: "



POTATO

Secure connection using key "4538538374224"  
User Meg wants these 6 letters: POTATO. User  
ida wants pages about "irl games". Unlocking  
secure records with master key 5130985733435  
Alice (browser) sends this message: "



# XKCD explanation

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "BIRD" (4 LETTERS).



User Olivia from London wants pages about "bees in car why". Note: Files for IP 375.381.83.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 34 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ccb9ff891-d3b-ff8)



HMM...



BIRD

User Olivia from London wants pages about "bees in car why". Note: Files for IP 375.381.83.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 34 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ccb9ff891-d3b-ff8)



# XKCD explanation

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

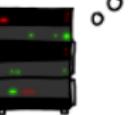
Memory Leak

Conclusion

SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "HAT" (500 LETTERS).

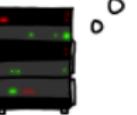


connection. Jake requested pictures of deer.  
User Meg wants these 500 letters: HAT. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHeBaSt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHeBaSt". User

connection. Jake requested pictures of deer.  
User Meg wants these 500 letters: HAT. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHeBaSt". User



Heartbleed,  
Technical  
Overview

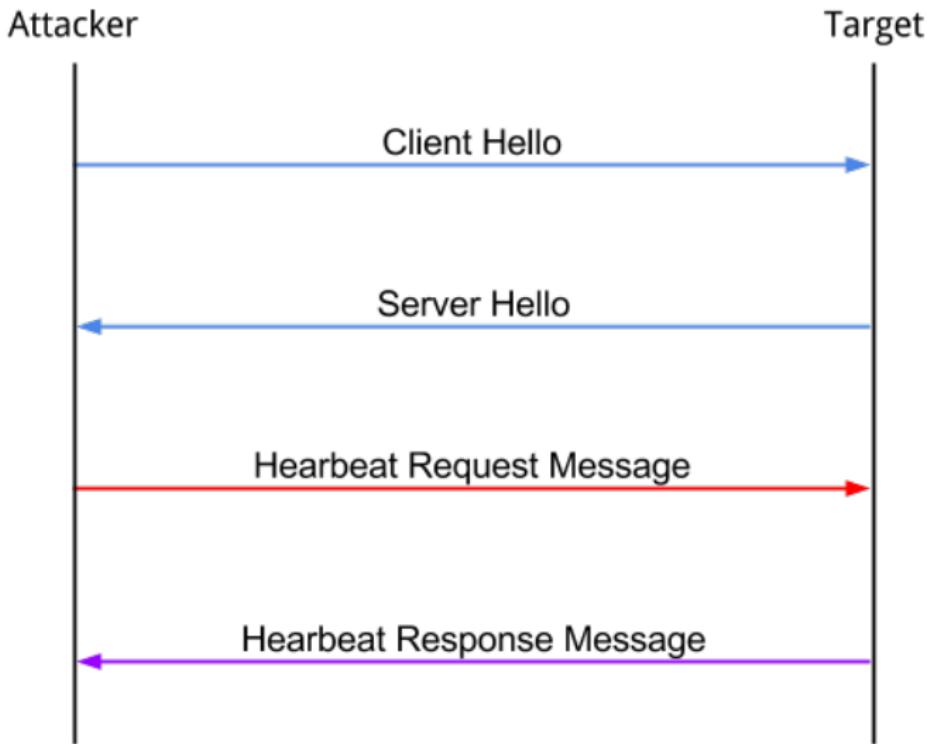
Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion



Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

## 3 Memory Leak

# Risk ?

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

- HTTP Headers
- Private Key
- Possibly anything from the server memory...

- It's possible but unlikely to have directly the RSA Private Key as it in the memory
- For encrypting a message OpenSSL use the struct RSA:

# RSA struct

```
struct rsa_st
{
    int pad;
    long version;
    const RSA_METHOD *meth;
    ENGINE *engine;
    BIGNUM *n;
    BIGNUM *e;
    BIGNUM *d;
    BIGNUM *p;
    BIGNUM *q;
    BIGNUM *dmp1;
    BIGNUM *dmq1;
    BIGNUM *iqmp;
    CRYPTO_EX_DATA ex_data;
    ...};
}
```

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

- p and q prime numbers
- $n = pq$  modulus
- $\varphi(n) = n - (p + q - 1)$
- e (public key exponent),  $1 < e < \varphi(n)$  and  $\gcd(e, \varphi(n)) = 1$
- d (private key exponent),  $d \equiv e^{-1} \pmod{\varphi(n)}$
- n and e are the public key, n and d are the private
- d, p, q,  $\varphi(n)$ , must be private
- if we get p or q it's a win

# Leaking p

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

- $p$  is a prime number and divide the modulus
- from the public key we have the size of  $p$
- scan the memory for a number which divide the modulus

# Why not found earlier ?

- OpenSSL code is extremely complex
- Static analysis of pointers, function pointers... is complex
- Over-read vulnerability is not the most common things to look for
- OpenSSL has its own memory allocation routines

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion

## 4 Conclusion

# Conclusion

Introduction

Heartbleed

Memory Leak

Conclusion

- "Everything" is impact
- Patch is not enough
- Firefox, Chrome, Opera don't use OpenSSL except on Android
- Lot's of tools will find it now
- Really interesting articles and research after this
- Lot's of review in OpenSSL since that

# Bibliography

- <http://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=96db902>
- <http://tools.ietf.org/html/rfc6520>
- <http://heartbleed.com/>
- <https://github.com/einaros/heartbleed-tools>
- <https://hacking.ventures/rsa-keys-in-heartbleed-memory/>
- <http://www.lightbluetouchpaper.org/2014/04/25/heartbleed-and-rsa-private-keys/>
- <http://blog.trailofbits.com/>
- <http://www.leviathansecurity.com/blog/leviathans-mandatory-heartbleed-blog-entry/>
- <http://www.dwheeler.com/essays/heartbleed.html>
- <https://filippo.io/Heartbleed/>
- ...

Heartbleed,  
Technical  
Overview

Bruno Pujos

Introduction

Heartbleed

Memory Leak

Conclusion