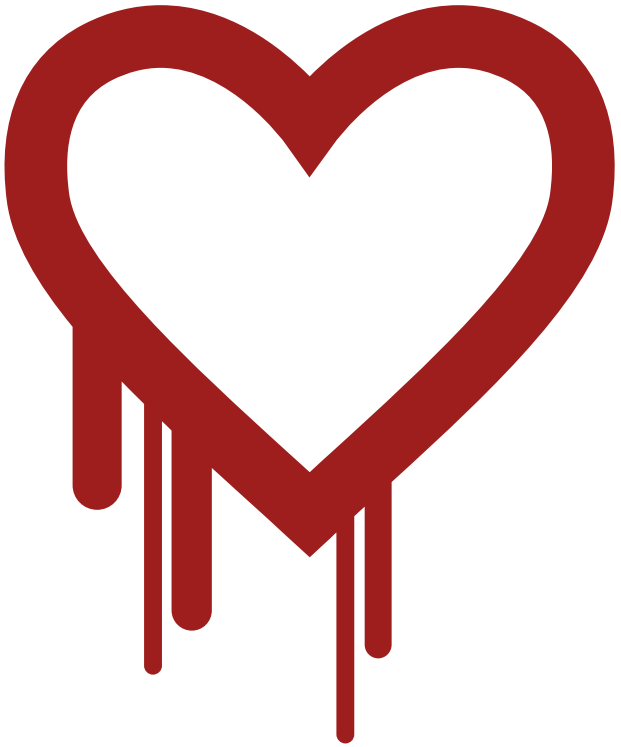
Heartbleed – Was war da eigentlich los?



TLS und Heartbeat

- RFC 6520 »TLS and DTLS Heartbeat Extension«
- Gedacht für MTU-Erkennung und keep-alive
- Heartbeat-Paket besteht aus Länge und Payload
- Unterstützung am 31. Dezember 2011 eingereicht
  - OpenSSL Version 1.0.1
- Heartbleed-Bug am 3. April 2014 entdeckt
- http://heartbleed.com am 7. April geschaltet

Das Heartbeat-Paket

```
/* nach RFC 6520 */
struct {
    int type;
    short payload_length;
    char payload[HeartbeatMessage.payload_length];
    char padding[padding_length];
} HeartbeatMessage;
```

- Sender darf beliebigen Payload mitschicken
- Empfänger senden selben Payload zurück
- Payload bis zu 2^{14} = 16384 Bytes lang

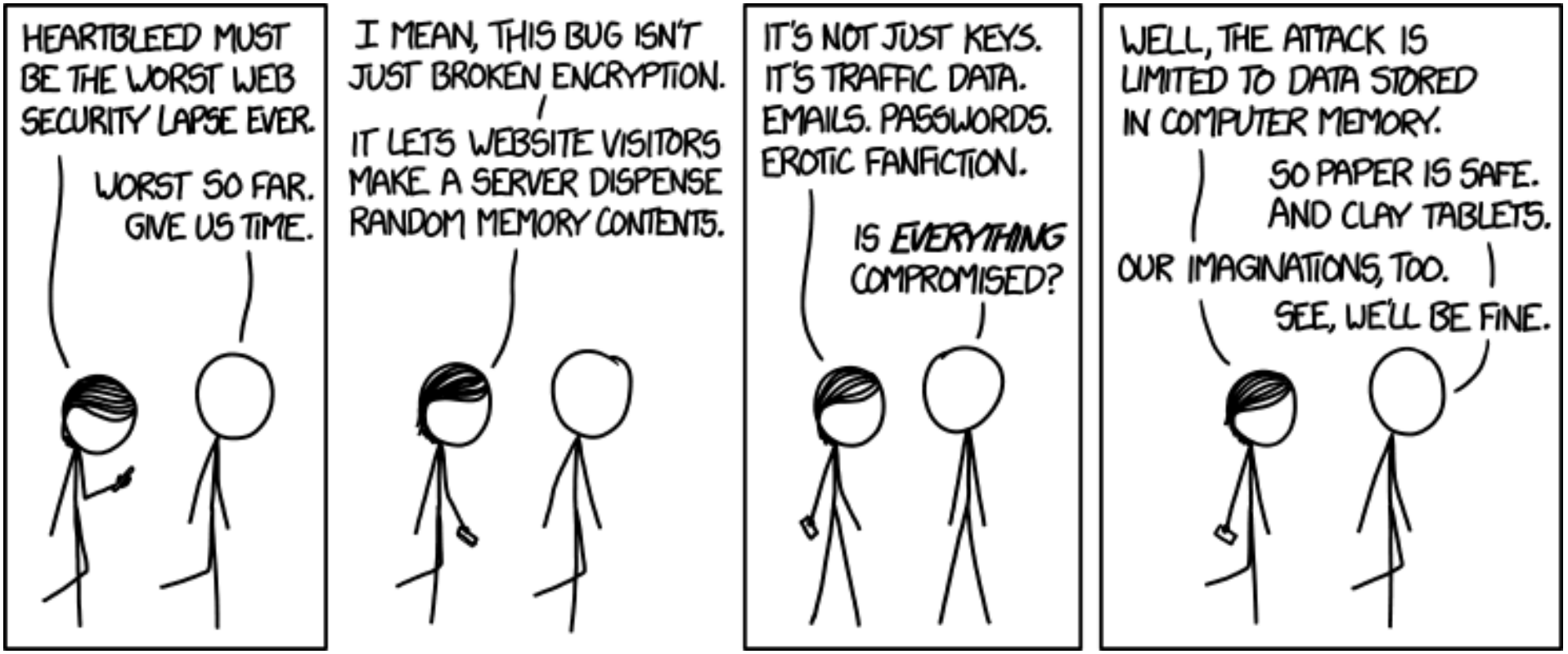
Die Umsetzung

- OpenSSL-Commit 4817504d069b4c5082161b02a22116ad75f822b1
- OpenSSL prüft `payload_length` nicht
- Was, wenn `payload_length` länger als das Paket ist?
- Speicherinhalt hinter Paketpuffer wird versendet
- Hauptspeicherinhalt wird dem Angreifer bekannt
- Erklärung in xkcd Nr. 1354

Wie wird das ausgenutzt?

- Hauptspeicher enthält interessante Daten
  - Schlüssel, Nutzerdaten, Zertifikate, Paßwörter
- Jedes Paket liefert andere Speicherteile zurück
- Hauptspeicher kann zusammengepuzzlet werden
- Angreifer kann Daten auslesen
- Verschlüsselung kann gebrochen werden
- Angriff geschieht unbemerkt

Warum ist das so eine Katastrophe?



xkcd Nr. 1353 © 2014 Randall Munroe (cc-by-nc 2.5)

Was muß getan werden?

- (Fast) jeder Dienst ist betroffen
- Vorsicht ist besser als Nachsicht

In dieser Reihenfolge:

1. OpenSSL-Bibliotheken austauschen
   - Versionen 1.0.1 bis 1.0.1f betroffen
2. Neue Schlüssel für betroffene Server
3. Neue Zertifikate für betroffene Server
4. Neue Paßwörter für alle Webdienste

Wie konnte das alles passieren?

»Catastrophic is the right word. On the scale of 1 to 10, this is an 11.«

– Bruce Schneier

- Sehr schlechte Qualität des OpenSSL-Quelltextes
- Wenige Menschen verstehen diesen
- Viele zweifelhafte Optimierungen
- Systematische Fehlersuche unmöglich

Tod durch `malloc(3)`

»OpenSSL is not developed by a responsible team.«

– Theo de Raadt, OpenBSD

- Eigene Speicherallokation pfercht Objekte zusammen
- Heartbleed auf OpenBSD dadurch erst möglich
- OpenSSL-`malloc()` im Prinzip abschaltbar
- Abschaltung funktioniert seit langem nicht mehr

LibreSSL

- OpenBSD-Fork genannt LibreSSL
- Massive Aufräumaktion durch OpenBSD
- Arbeit begann unmittelbar nach Heartbleed
- Umschreibung des Codes für größere Sicherheit
- Entfernung von Altlasten
  - 90 000 Zeilen C-Code und 150 000 Zeilen sonstiges
  - Dual_EC_DRBG, MD2, SSL v2, Kerberos, J-PAKE, SRP
  - OpenSSL umfasst ca. 530 000 Zeilen Code und Text