Heartbleed

Lite smått och gott om heartbleedbuggen

Robert Malmgren
rom@romab.com
https://www.romab.com

Upplägg

- Vad är heartbleed?
- Vad är OpenSSL?
- Vad är konsekvenserna av heartbleed?
- Var kan heartbleed finnas?
- Heartblead i jämförelse med annat?
- Vad skall man göra?

Vad är heartbleed?

- En bugg i programvarupaketet OpenSSL
- Det går via nätverk nå webbserverar som påverkas att *läcka minne* och skicka tillbaka detta som svar över nätverket
    - Minnesläckan med tillhörande informationsläckage är ett allvarligt säkerhetsproblem
- Buggen har funnits i OpenSSL mellan december 2011 och april 2014 (~2,5 år) i version 1.0.1-releaser

Vad är OpenSSL?

- Programvarupaketet OpenSSL implementerar protokollet SSL/TLS och de kryptofunktioner som tillhör detta
    - OpenSSL är öppen källkod
    - OpenSSL drivs av OpenSSL-projektet
    - Frivilliga som utvecklar kod
    - OpenSSL ingår som modul i väldigt många andra programpaket
        - Webbservrar: Apache, nginx, mfl
        - Är lib (kodbibliotek) som byggs in och används av många andra program
        - är kommandoradsverktyg som nyttjas från script, etc

Vad är heartbleed?

- En bugg i implementationen av tillägget “heartbeat” till standarden TLS

- *RFC 6520 “Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension”*

- *Upp till 64kb information kan läcka vid varje försök*

    - *Möjliggör att någon repetitivt frågar och får svar med nya minnesdumpar*

Illustration av attacken (1/3)

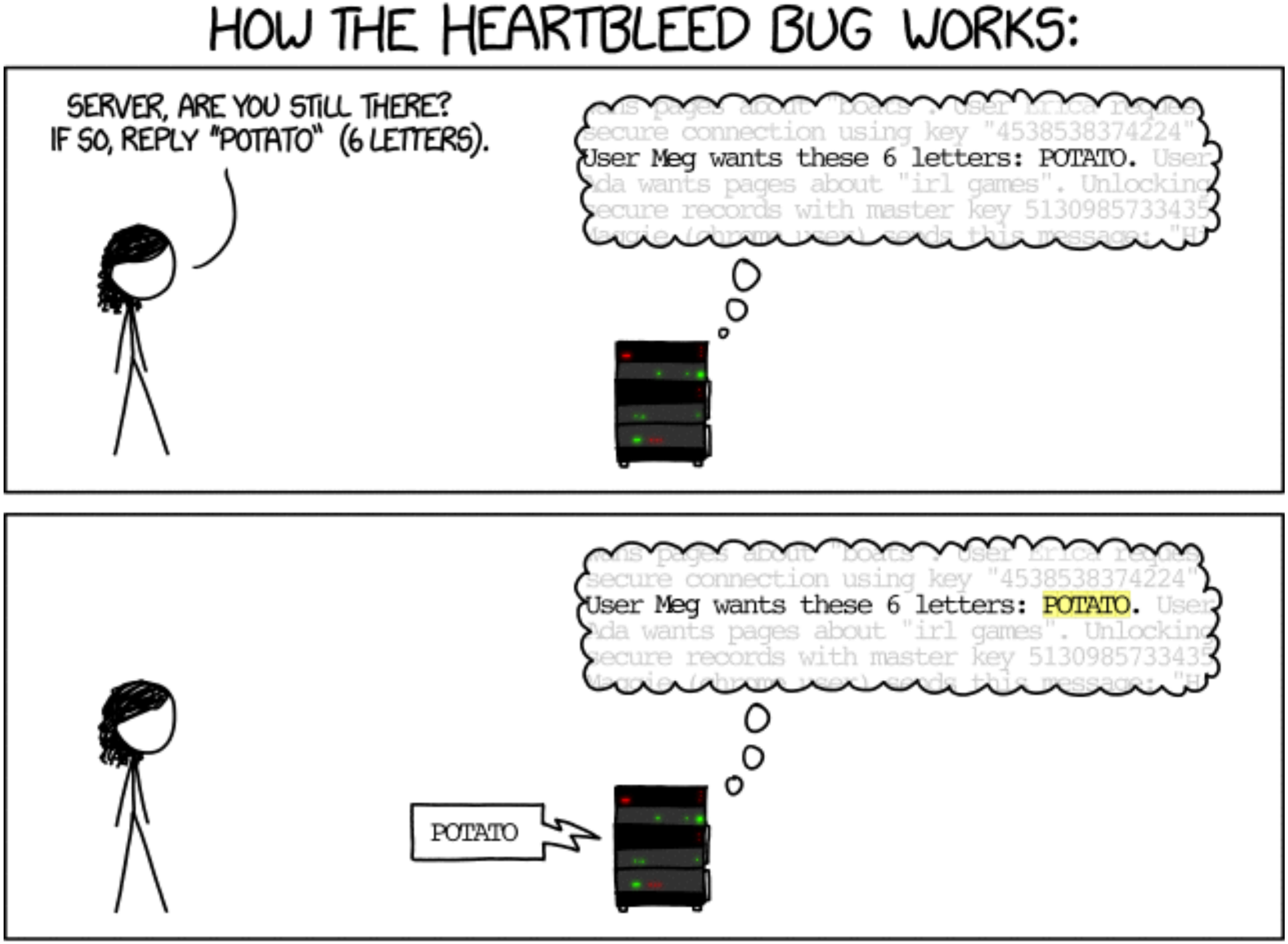


Illustration av attacken (2/3)

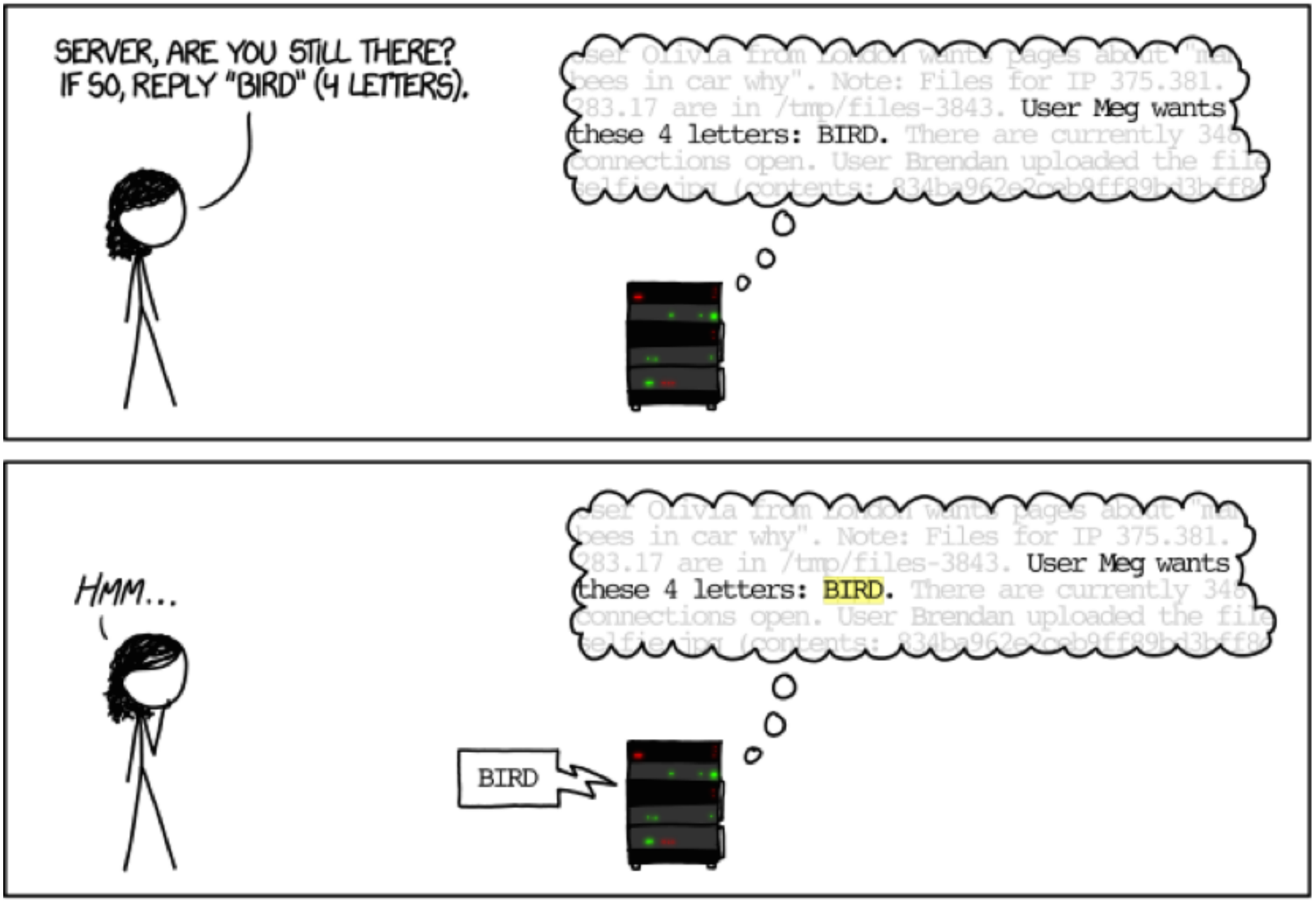
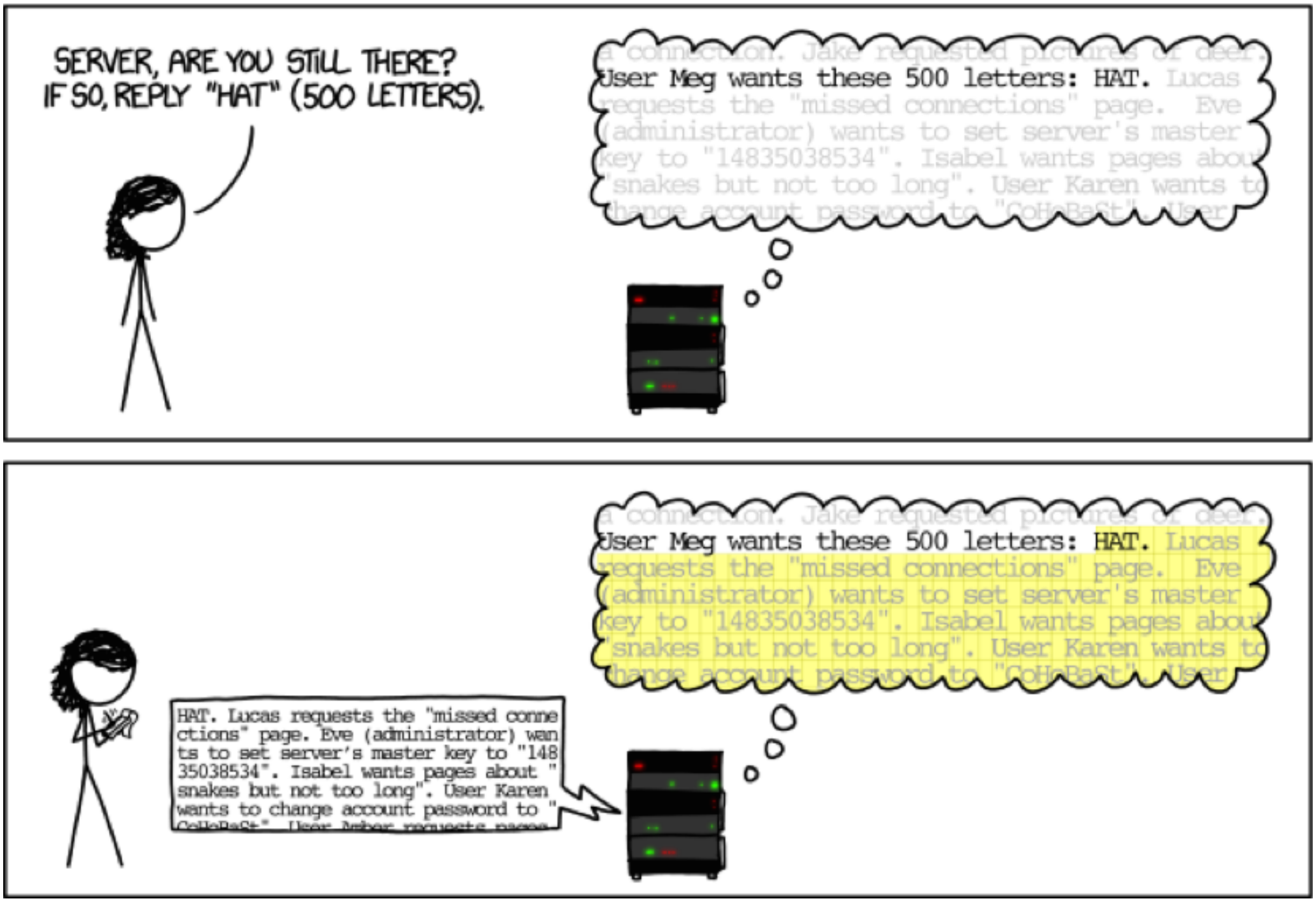


Illustration av attacken (3/3)



Vad är konsekvenserna av heartbleed?

- Skräckexemplet - informationsläckage av (privata) kryptonycklar som hör till SSL/TLS
- Annat som fanns i aktuell minnesarea:
    - åtkomstskyddade webbsidor, “privata webbsidor”, chatt, mail, mm
    - applikationsdata, programkod/skript
    - användarnamn, lösenord

Var kan heartbleed finnas?

- Webbplatser
- VPN-lösningar (OpenVPN)
- Serverprogram som använder sig av SSL/TSL: epost, IM (chatt)
- Säkerhetslösningar som använder sig av SSL/TLS: **Tor**
- Klientprogram som använder sig av OpenSSL
- Appar och serverback-end som håller ihop med appen
- Hemmaroutrar, kommunikationsutrustning
- Inbyggda system

Hur förhåller sig heartbleed till andra säkerhetshål?

- Motsvarande konsekvenser med informationsläckage skulle kunna inträffat om
    - det fanns en pluginmodul till webservern med hål
    - buggar i serverprogram (webb, sökmotor)
    - buggar i TCP/IP-stacken, ethernet driver,
    - etc
- det finns historiska exempel på ovanstående
- Andra SSL-buggar, andra SSL-implementationer

Vad är status?

- Det finns buggfixar till OpenSSL. Version 1.0.1g är lagad
- Många stora webbplatser har patchat sina plattformar
- Det finns ett antal attackverktyg i omlopp: skripts, mer avancerade verktyg
- Det har skett ett antal stölder av lösenord

Problem och kritik (1/2)

- Underfinansierad infrastrukturkomponent som alla beror på
    - Detta kanske har löst sig som en effekt av heartbleed!
- Kritik mot kodkvaliteten
    - Mycket legacykod, mycket kod för portabilitet till olika datorarkitekturer och olika operativsystem
    - OpenBSD har gjort en fork - libressl - som främst är bortstädning av gammal kod

Problem och kritik (2/2)

- Kritik och förvirring kring “varningsprocessen”
    - Vem hittade hålet? Vaddå “parallella upptäckter”?
    - Många CERT-organisationer, OS-leverantörer, mfl fick varningen väldigt sent
    - Lång stund oklarheter, förvirring, osäkerhet hur allvarligt buggen var
- Var hålet känt sen tidigare?

Andra problem

- Webbservrar med äldre versioner OpenSSL är inte sårbara för heartbleed
    - Värt att tänka på om man “testar med testverktyg mot webbservern”
        - Men det finns andra buggar i dessa gamla versioner, som inte detekteras
- Man kan ha flera versioner av OpenSSL installerad i sitt system!
    - Statiskt inkompilerad, olika beroenden i pakethanterare, kod som inte sköts via pakethanteringen, etc

Vad skall man göra?

Webbplatsinnehavare

- Uppgradera OpenSSL
- Patcha sina program som använder OpenSSL
- Testa sin server om fixen tagit
- Byta X.509-certifikat
- Informera användare
- Byta lösenord

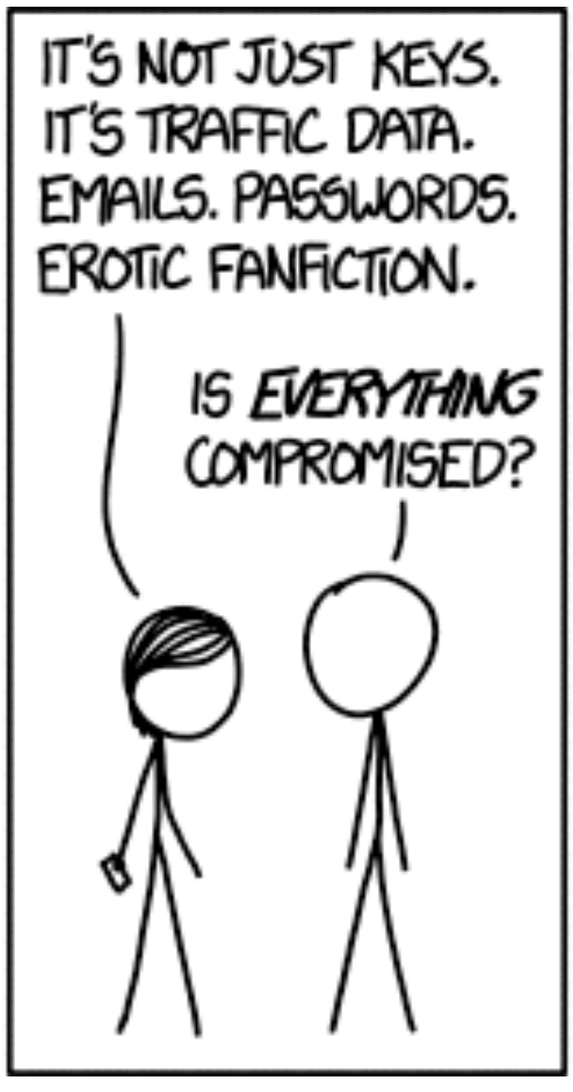
Användare

- Se ifall något program man använder måste uppgraderas
- Tänka igenom vilka tjänster man använder
- Bråka med (webb) platsleverantörer om uppgraderingar
- Byta lösenord

Sammanfattning

- Vi kommer få höra om Heartbleed och dess effekter lång tid framöver
- Allvarlig bugg som påverkar mycket på Internet
- Det finns mycket att göra som användare/ webbinnehavare

Sammanfattning (grafisk)



Mer information

- Startsida för information http://heartbleed.com/
- OpenSSLs information om heartbleed
  - https://www.openssl.org/news/secadv_20140407.txt
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
- https://xkcd.com/1353/
- https://xkcd.com/1354/
- http://www.libressl.org/
- https://www.ssllabs.com/ssltest/
- https://filippo.io/Heartbleed/
- https://www.eff.org/deeplinks/2014/04/bleeding-hearts-club-heartbleed-recovery-system-administrators