FACULTEIT INGENIEURSWETENSCHAPPEN

Network and Computer Security

Chapter 1 - Introduction

Prof. dr. ir. Eli De Poorter

Overview

- Security in the media
- Recent major incidents
  - Heartbleed (2014)
  - Sony Pictures Entertainment hack (2014)
  - Ashley Madison (2015)
  - Others
- Why do we need security?
- Scope of the course

What comes to mind when you hear the term “Security”?

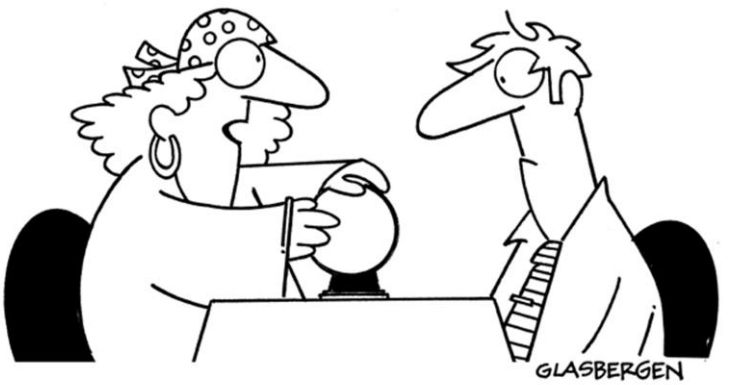
What are we talking about?

- A few examples from the news
  - "Social engineering", Internet fraud, etc.
  - Hackers
  - Password security
  - Privacy
  - Security of confidential information
  - Cybercrime, cyberterrorism, cyberwar, etc.
  - Malware…
    - …now also for MacOS and Android
  - Did we mention the NSA?

Overview

- **Security in the media**
- **Recent major incidents**
- **Why do we need security?**
- **Scope of the course**

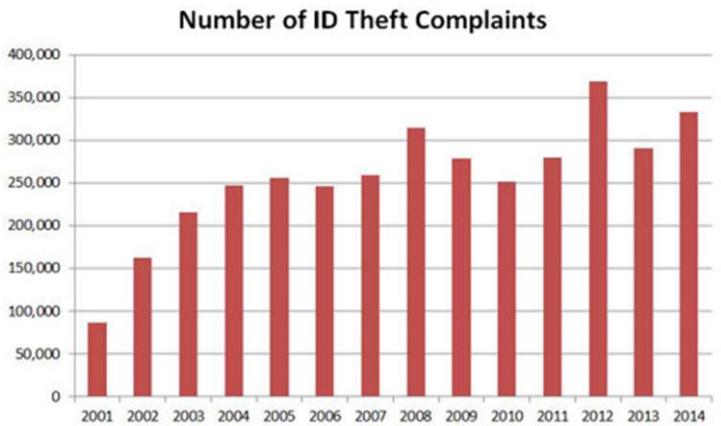
The rise of social networks



"I can't see your future, but I found your bank files, Social Security number and all of your company passwords."

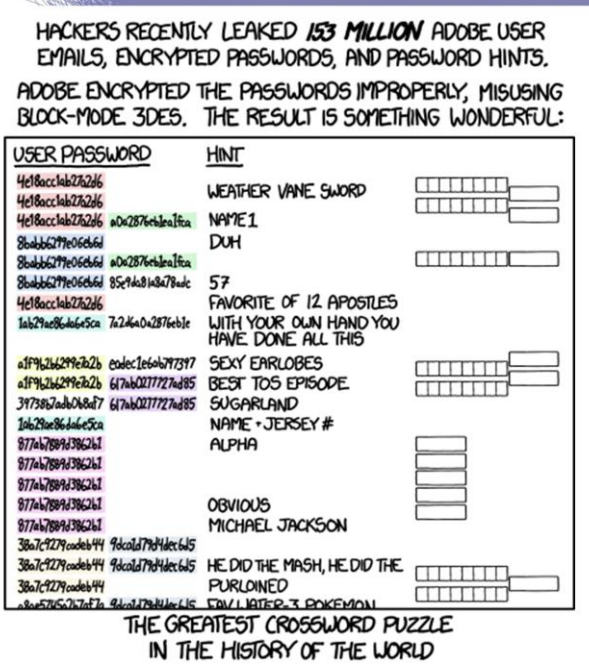
Your Identity Is Worth $5 on the Black Market
In other words, significantly less than it's worth to you….

http://newsfeed.time.com/2013/08/26/your-identity-is-worth-5-on-the-black-market/



http://www.idtheftawareness.com/id_theft_pages/WhatIsIdTheft.php

You'll never walk alone (1)



http://xkcd.com/1286/

Adobe 2013

source: xkcd.com

You'll never walk alone (2)

Insurance giant Anthem hit by massive data

CNN Money

2015-02-05

http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/index.html

Personal data in database not always secure

DE REDACTIE.BE

Persoonlijke gegevens in databases niet altijd veilig

2014-10-16

http://deredactie.be/permalink/1.2120513

Apple to beef up security measures after nude photo leak

CNN Money

2014-09-04

http://money.cnn.com/2014/09/04/technology/security/apple-celebrity-photos/

Bitcoin bank Flexcoin closes after hack

theguardian

2014-03-04

http://www.theguardian.com/technology/2014/mar/04/bitcoin-bank-flexcoin-closes-after-hack-attack

Clearly not the only issue with bitcoin last year

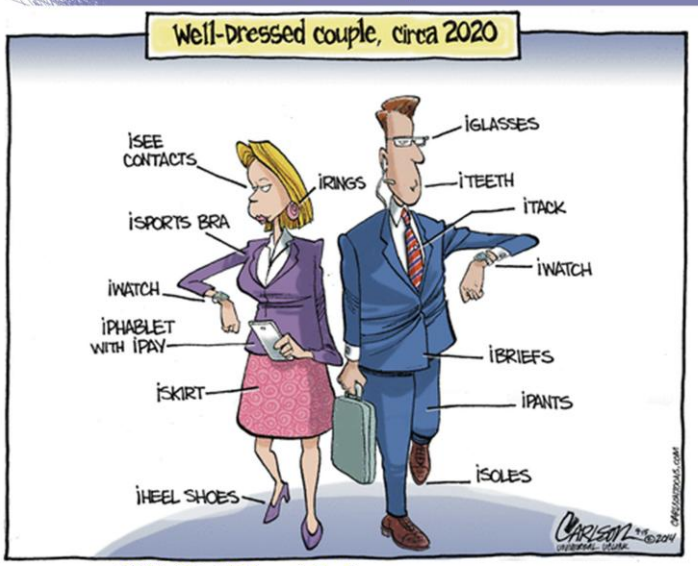
Cheney's defibrillator was modified to prevent hacking

CNN

2013-10-24

http://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/

Think of what IoT promises



2014-09-15 Stuart Carlson

washingtonpost.com

Russian Hackers Amass Over a Billion Internet Passwords

The New York Times 2014-08-05

http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials

Why I Am Skeptical About 1.2 Billion Passwords Being Stolen

Forbes 2014-08-07

http://www.forbes.com/sites/josephsteinberg/2014/08/07/why-i-am-skeptical-about-1-2-billion-passwords-being-stolen/

Russian Hackers Amass Over a Billion Internet Passwords

The New York Times 2014-08-05

http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

So you think you're safe?

NSA hacks Belgian cyberprof

NSA hackt Belgische cyberprof

De Standaard

2014-01-31

http://www.standaard.be/cnt/dmf20140131_049

Rise of the "securocrats"…

- A bit too much for a single article…
  - …so let's have a full section in the newspaper
    - 1833 articles (2015-02-09 10:00) and counting…

NSA

The latest news and comment on the US National Security Agency

theguardian

Since 2013-06-06

http://www.theguardian.com/us-news/nsa

- Remain a critic, remain a sceptic
  - Journalists aren't always exactly IT experts!

“Defending Our Nation”?

2013-12-20 Tom Toles

washingtonpost.com

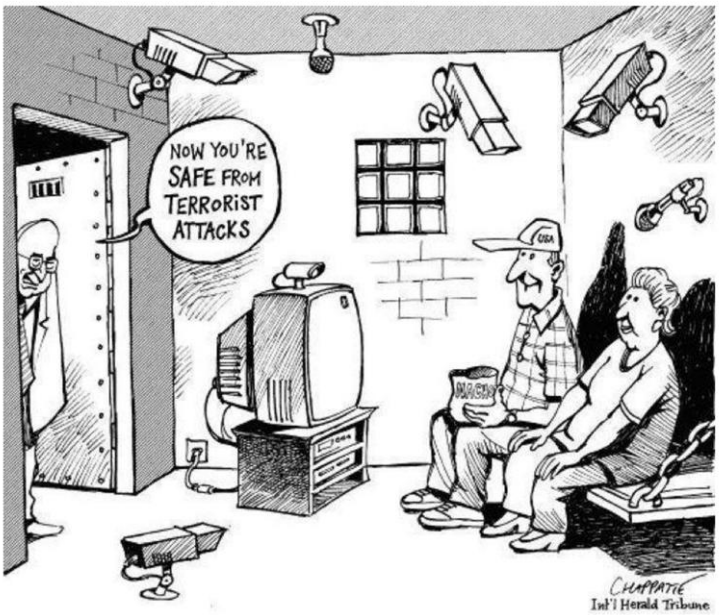
WAR IS PEACE

FREEDOM IS SLAVERY

IGNORANCE IS STRENGTH

George Orwell, “1984”

The cost of security?



http://www.prosebeforehos.com/political-ironing/01/03/national-security-america/

Irony?

Well, actually this is just a hoax

Not just the NSA

NSA hacks Internet forums, 'against law'

AIVD hackt internetfora, 'tegen wet in'

NRC HANDELSBLAD 2013-11-30

http://www.nrc.nl/nieuws/2013/11/30/aivd-hackt-internetfora-tegen-wet-in/

Revelations about the French Big Brother

Révélations sur le Big Brother français

Le Monde.fr 2013-07-04

http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

British intelligence hacked Belgian telephone company

Britischer Geheimdienst hackte belgische Telefongesellschaft

DER SPIEGEL 2013-09-20

http://www.spiegel.de/netzwelt/web/belgacom-geheimdienst-gchq-hackte-belgische-telefongesellschaft-a-923224.html

Consequences?

Here's what can go wrong when the government builds a huge database about Americans

washingtonpost.com

2013-07-08

http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/08/heres-what-can-go-wrong-when-the-government-builds-a-huge-database-about-americans/

Every single IT guy, every single manager…

CROOKED TIMBER (blog)

2014-09-23

http://crookedtimber.org/2014/09/23/every-single-it-guy-every-single-manager/

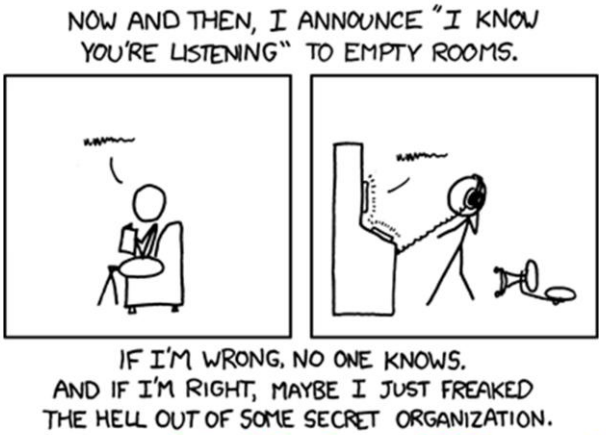
Quis custodiet ipsos custodes?
(Juvenalis, Satire 6.346–348)

Consequences?

2013-10-31 Ben Sargent

washingtonpost.com

Consequences?



http://xkcd.com/525/

Source: xkcd.com

And corporations aren't any better

Facebook signs users up to privacy policy that allows it to track you everywhere on the internet

The INDEPENDENT 2015-02-04

http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-signs-users-up-to-privacy-policy-that-allows-it-to-track-you-everywhere-on-the-internet-10022530.html

Does Uber Even Deserve Our Trust?

Forbes 2014-11-25

http://www.forbes.com/sites/chanellebessette/2014/11/25/does-uber-even-deserve-our-trust/

Apple pushes out first-ever automatic security upgrade for Mac

CNN Money 2014-12-23

http://money.cnn.com/2014/12/23/technology/security/apple-automatic-security-upgrade/index.html

Number of viruses on Android smart phones increases spectacularly

Aantal virussen op Android-smartphones stijgt spectaculair

DeMorgen. 2013-11-27

http://www.demorgen.be/technologie/aantal-virussen-op-android-smartphones-stijgt-spectaculair-a1748265/

An intractable problem?

Internet bank fraud increased by 70% in 2013

DE REDACTIE.BE

Fraude met internetbankieren steeg met 70% in 2013

2014-02-10

http://www.deredactie.be/permalink/1.1869606

Number of Internet bank fraud cases strongly decreased

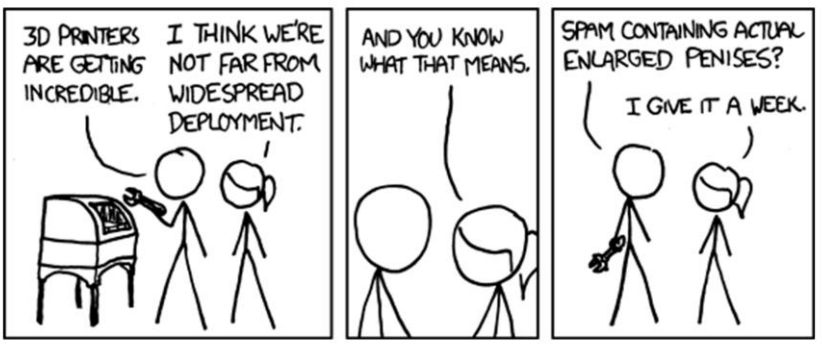
DE REDACTIE.BE

Aantal fraudegevallen met internetbankieren daalt sterk

2015-01-30

http://deredactie.be/permalink/1.2223667

In your mailbox…



http://xkcd.com/924/

Source: xkcd.com

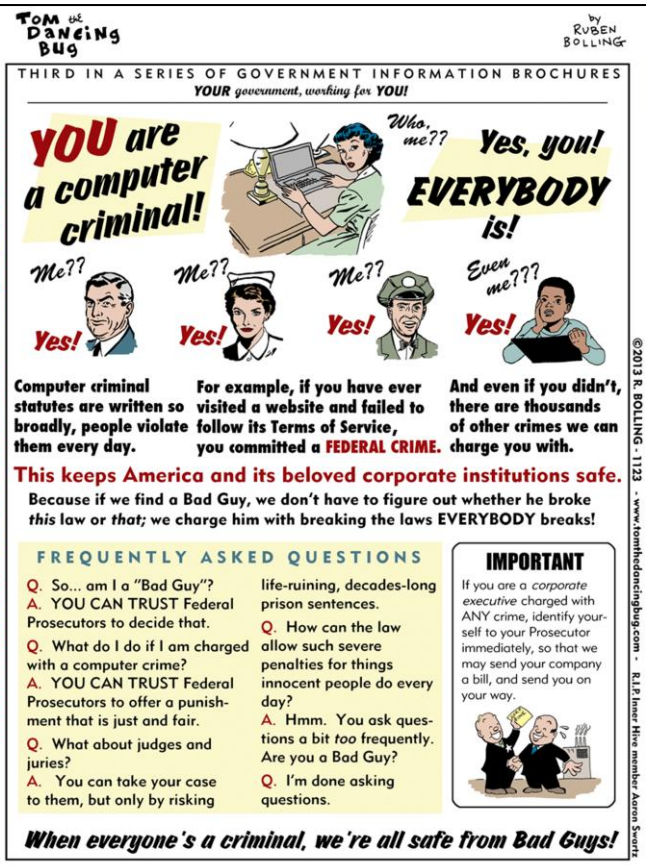
Hackers of the world…

http://xkcd.com/932/

Source: xkcd.com

http://boingboing.net/2013/01/30/tom-the-dancing-bug-you-are.html

Source: dailykos.com



Hypes?

- **Cyberterror our main preoccupation?**

2004-06-01 Tom Toles

washingtonpost.com

Hypes?

- **Cyberterror our main preoccupation?**

2015-01-15 Signe Wilkinson

washingtonpost.com

There goes the 768 bits key

http://archives.lesoir.be/festin-sous-marin-cryptographie-exit-la-cle-de-768-bits_t-20100109-00RQKV.html

Largest prime number ever discovered

http://www.deredactie.be/permalink/1.1542554

33

Grootste priemgetal: 2^57885161-1 (17425170 decimale digits)

The eternal dilemma

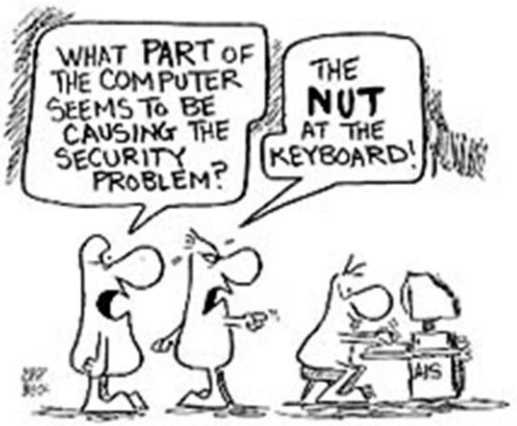
- **Secure or user-friendly?**

2009-02-03 On the Fastrack

washingtonpost.com

And in conclusion…

- …the human factor



LA Times

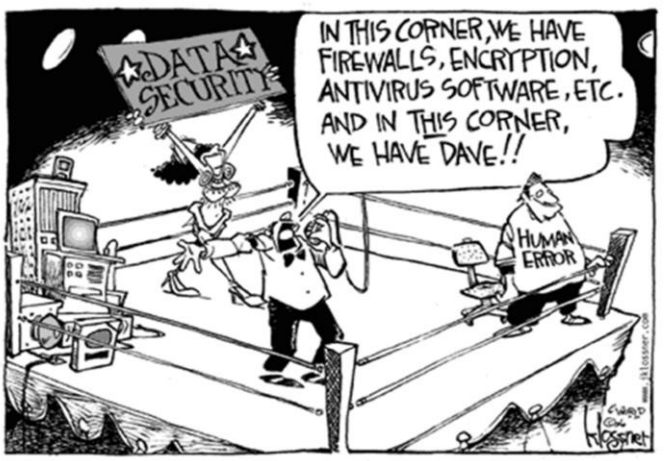
1 in 10 in a survey think HTML is an STD

2014-03-04

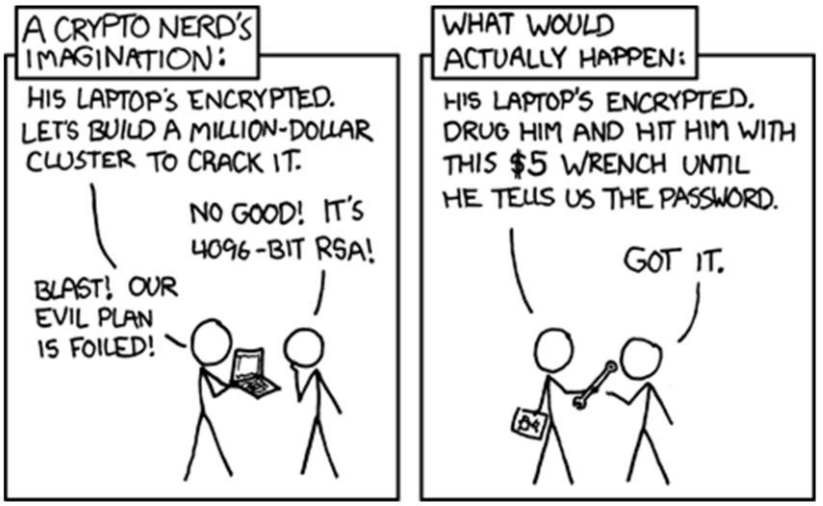
http://www.latimes.com/business/technology/la-fi-tn-1-10-americans-html-std-study-finds-20140304-story.html

And in conclusion…

- …the human factor



Non-technological…



Source: xkcd.com

http://xkcd.com/538/

Overview

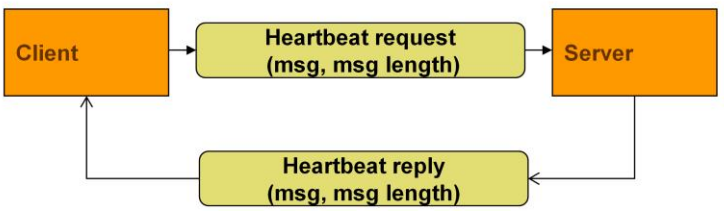
- Security in the media
- Recent major incidents
  - **Heartbleed (2014)**
  - Sony Pictures Entertainment hack (2014)
  - Ashley Madison (2015)
  - Others
- Why do we need security?
- Scope of the course

What is Heartbleed?

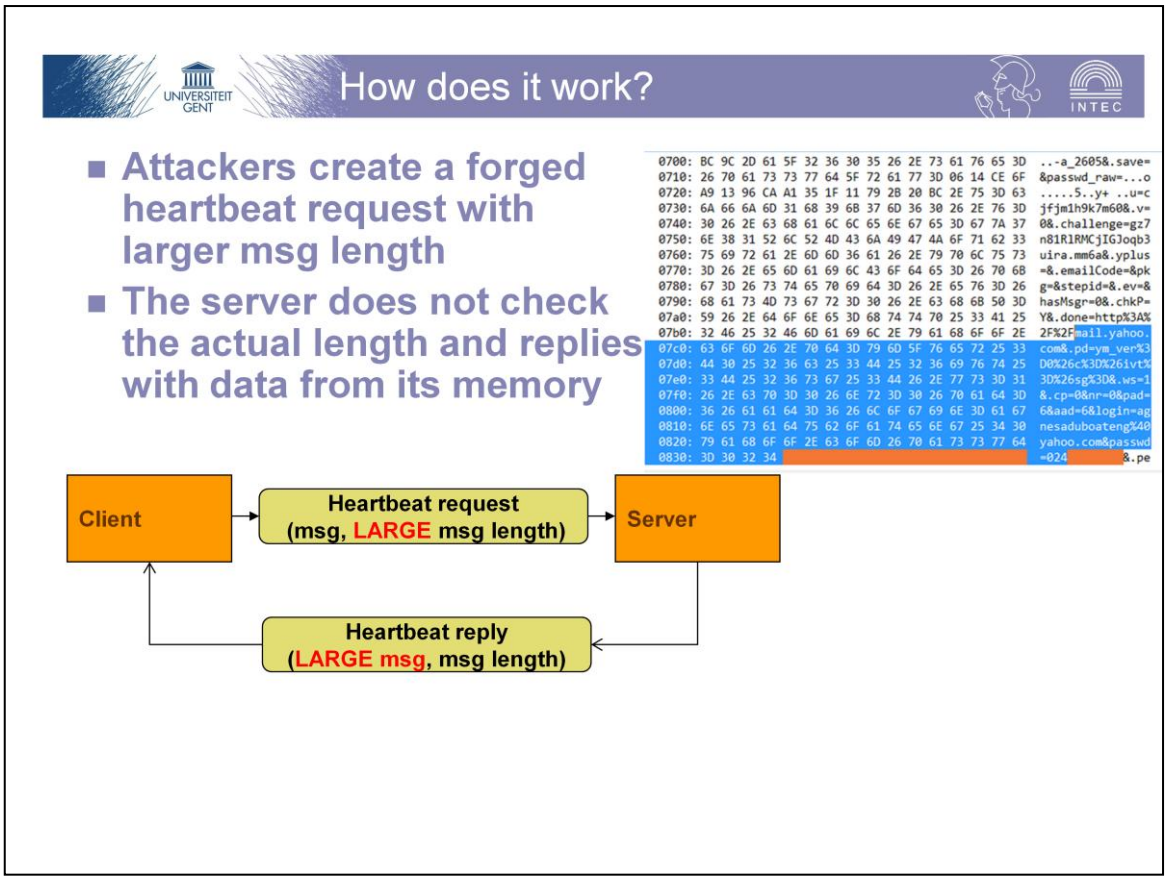
- **Heartbleed is a vulnerability in OpenSSL software.**
- **OpenSSL is encryption software that accesses websites through a "secure" connection**
  - **E.g. HTTPS://.**
- **Https uses SSL or TLS for encrypting sensitive data**
  - **Banking, e-shopping, etc.**
  - **A heartbeat is send regularly to check if the other party is alive**
    - For efficiency (to avoid setting up a new connection)
    - For safety (to check if we can still communicate)
- **Heartbeat**
  - **Short block of data + length of the data**

How does it work?

- **Heartbeat: keep alive a secure TLS connection**



The Heartbeat Extension for the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols was proposed as a standard in February 2012 by RFC 6520. It provides a way to test and keep alive secure communication links without the need to renegotiate the connection each time. The RFC 6520 Heartbeat Extension tests TLS/DTLS secure communication links by allowing a computer at one end of a connection to send a "Heartbeat Request" message, consisting of a payload, typically a text string, along with the payload's length as a 16-bit integer. The receiving computer then must send exactly the same payload back to the sender.



The affected versions of OpenSSL allocate a memory buffer for the message to be returned based on the length field in the requesting message, without regard to the actual size of that message's payload. Because of this failure to do proper bounds checking, the message returned consists of the payload, possibly followed by whatever else happened to be in the allocated memory buffer. Heartbleed is therefore exploited by sending a malformed heartbeat request with a small payload and large length field to the vulnerable party (usually a server). The malformed block says its length is 64KB, the maximum possible. The server copies that much data from memory into the response, permitting attackers to read up to 64 kilobytes of the victim's memory that was likely to have been used previously by OpenSSL. This memory is likely to contain sensitive information, such as passwords or even the public or private key information. Since the attack is not logged in the server database, attackers can use this bug undetected. Since the contents of the memory change over time, the attack can be performed multiple times to gradually obtain more information. Moreover, the obtained information can even be used to decrypt message exchanges from the past.

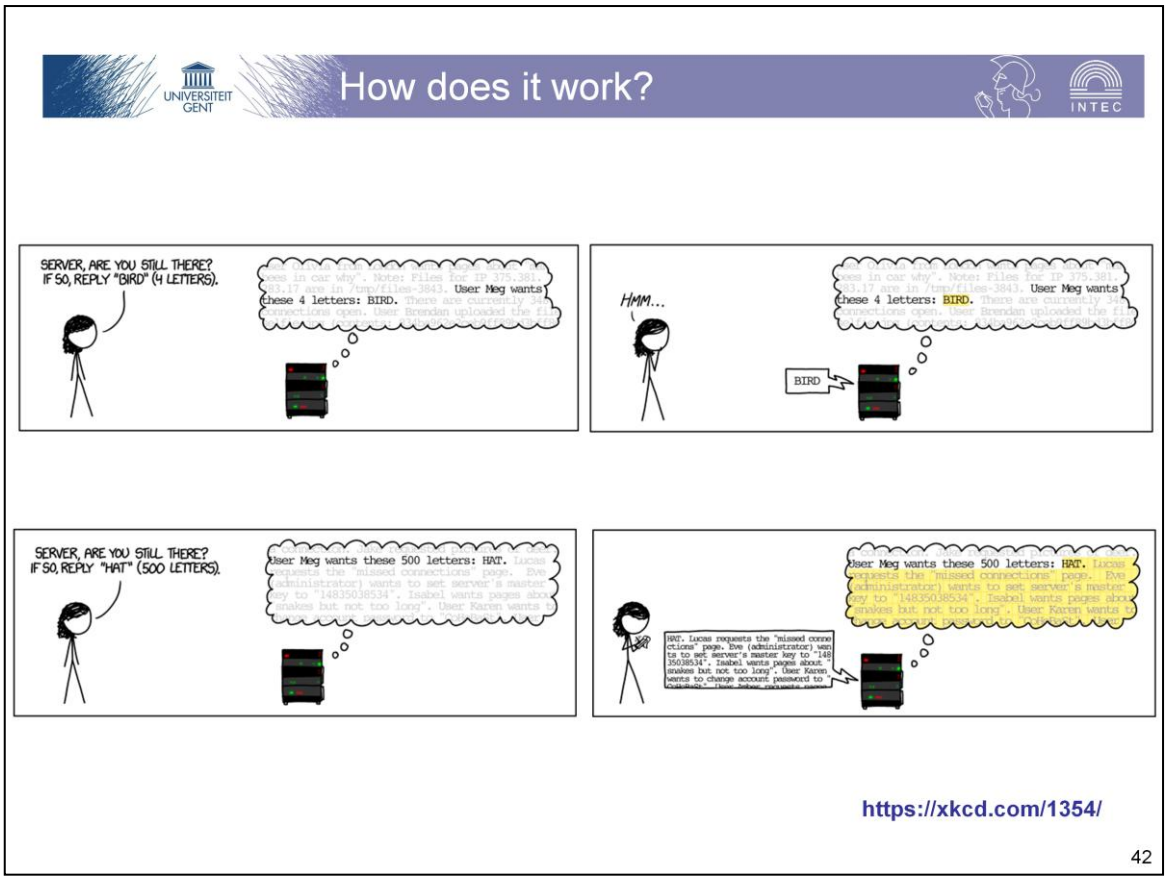
Note that heartbleed is not a flaw in TLS: it is a simple memory safety bug in OpenSSL!

More information from

http://www.seancassidy.me/diagnosis-of-the-openssl-heartbleed-bug.html

http://blog.cryptographyengineering.com/2014/04/attack-of-week-openssl-heartbleed.html

https://vimeo.com/91425662 (video)



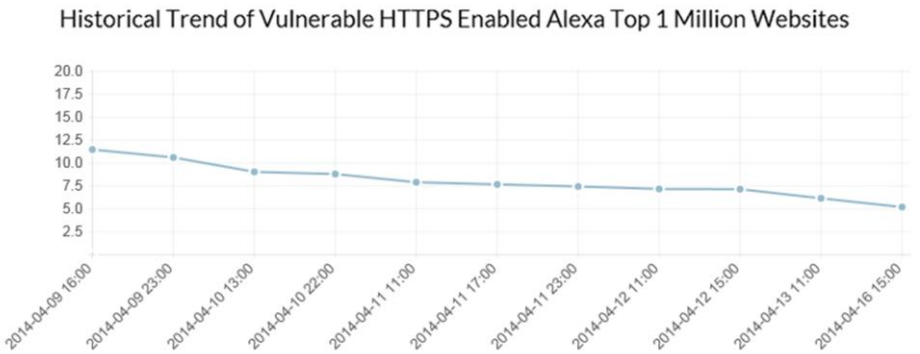
Where a Heartbeat Request might ask a party to "send back the four-letter word 'bird'", resulting in a response of "bird", a "Heartbleed Request" (a malicious heartbeat request) of "send back the 500-letter word 'bird'" would cause the victim to return "bird" followed by whatever 496 characters the victim happened to have in active memory. Attackers in this way could receive sensitive data, compromising the confidentiality of the victim's communications. Although an attacker has some control over the disclosed memory block's size, it has no control over its location, and therefore cannot choose what content is revealed.

When happened when?

OpenSSL released	March 2012
Patch released (Some fixes had already been put in place then)	21 March 2014
Publicly reported as vulnerable	1 April 2014
First proven attempted exploit	8 April 2014
Intentional vulnerability test	12 April 2014

How may sites are vulnerable?
(After vulnerability was reported publically)

When happened when?



A list the top 1,000 most popular web domains and mail servers that remain vulnerable.
https://zmap.io/heartbleed/

Overview

- Security in the media
- Recent major incidents
  - Heartbleed (2014)
  - **Sony Pictures Entertainment hack (2014)**
  - Ashley Madison (2015)
  - Others
- Why do we need security?
- Scope of the course

Sony Pictures Hack

- Hack into Sony Pictures
  - Perpetrators: The Guardians Of Peace (GOP)
  - Result
    - Crippled network, theft of valuable information, theft of unreleased materials
      - ✓ Employee data, network information, security information, payment information, …
  - Vague allegations North Korea is responsible in retribution for the imminent release of an upcoming movie titled “The Interview”.
    - Alternatives include former employees, China, Russia, …
- Clearly political motivated
  - Repeated releases, significant media attention

Sony Pictures Hacked And Blackmailed

Forbes 2014-11-24

http://www.forbes.com/sites/davelewis/2014/11/24/sony-pictures-hacked-and-blackmailed/

US tapped N Korean networks years ago, providing proof of Sony hack –

theguardian 2015-01-19

http://www.theguardian.com/film/2015/jan/19/us-tapped-n-korean-networks-years-ago-providing-proof-of-sony-hack-reports

FBI doubts North Korea link to Sony Pictures hack

theguardian 2014-12-10

http://www.theguardian.com/technology/2014/dec/10/fbi-doubts-north-korea-link-sony-pictures-hack

Overview

- Security in the media
- Recent major incidents
  - Heartbleed (2014)
  - Sony Pictures Entertainment hack (2014)
  - **Ashley Madison (2015)**
  - Others
- Why do we need security?
- Scope of the course

Ashley Madison data breach

- What?
  - A commercial website for enabling extramarital affairs
- Perpetrators: "The Impact Team“
  - Stolen items
    - Personal information from users, e-mails and corporate data
  - Demands
    - Shut down of the site
- Motivation
  - “ethical” hacking…?
- Results
  - Insights in falsified profiles
  - Broken marriages, several suicides
  - Damage up to …. millions?

50

Passwords on the live site were hashed using the bcrypt algorithm. A security analyst using the Hashcat password recovery tool with a dictionary based on the RockYou passwords found that among the 4,000 passwords that were the easiest to crack, "123456" and "password" were the most commonly used passwords on the live website. An analysis of old passwords used on an archived version showed that "123456" and "password" were the most common. Due to a coding error where passwords were hashed with both bcrypt and md5 11 million passwords were eventually cracked.

Overview

- Security in the media
- Recent major incidents
  - Heartbleed (2014)
  - Sony Pictures Entertainment hack (2014)
  - Ashley Madison (2015)
  - **Others**
- Why do we need security?
- Scope of the course

Major recent incidents

- Operation Aurora (2010)
- Australian cyberattacks (2010)
- Operation Payback (2010)
- HBGary Federal (2011)
- DigiNotar (2011)
- Operation Tunisia (2011)
- 2011 PlayStation Network outage (2011)
- Operation AntiSec (2011)
- Stratfor email leak (2012–13)
- LinkedIn hack (2012)
- South Korea cyberattack (2013)
- Snapchat hack (2013)
- Operation Tovar (2014)
- 2014 celebrity photo hack (2014)
- Heartbleed (2014)
- Shellshock (2014)
- POODLE (2014)
- Sony Pictures Entertainment hack (2014)
- Office of Personnel Management data breach (2015)
- Hacking Team (2015)
- Ashley Madison (2015)
- Stagefright (2015)
- ….
- To be continued….

52

All off the above incidents provide for insightful and entertaining reading material, in which both the technical aspects should be considered as well as the motivation behind the incidents. Most of them show how majorly technology and politics are entwined in current days.

Overview

- Security in the media
- Recent major incidents
- **Why do we need security?**
- Scope of the course

- **Why Information Security?**
  - **Counterpart of securing material objects**
    - **Material object have some value**
      - ✓ Value can often easily be determined (except for affective value)
    - **Can be stolen or damaged**
      - ✓ Causes material damage (replacement of the object, interruption of business process, etc.)
      - ✓ Most damage is repairable (replacement or repair)

- **Why Information Security?**
  - **Counterpart of securing material objects**
    - **Protecting from damage**
    - **Protecting from theft**
      - ✓ Locks, safes, etc.
    - **Cost for security/protection takes into account:**
      - ✓ Value of the object
      - ✓ Risk of theft/damage

- **Why Information Security?**
  - **Value of information**
    - **Sometimes hard to assess**
    - **Best estimated by damage caused**
      - ✓ When information security is breached
      - ✓ But even this can be hard:
        - » what is the value of someone's privacy?
  - **Threats against information**
    - **Loss of information**
    - **Forged information**
    - **Unauthorised release of information**
    - **Repudiation of information**
    - **etc.**

- **Why Information Security?**
  - **Consequences of security breaches**
    - **Can't always be undone**
      - ✓ Lost information
      - ✓ Unauthorised release of information
  - **Measures**
    - **Information security:**
      - ✓ encryption, digital signature, etc.
    - **Carry some cost**
      - ✓ Implementation, lost ease-of-use, etc.
    - **Here too, dependent on…**
      - ✓ …risk of security breach
      - ✓ …potential damage in case of breach

- **Why Information Security?**
  - **Value of information systems**
    - Also hard to assess
    - Systems are meant to enable some service
      - ✓ Damage when service is unavailable or unreliable
  - **Threats against information systems**
    - **Unavailability**/disruption of service
    - **Unauthorised access** to service
    - Threats against exchanged information
    - etc.

Why Information Security?

- **Security measures for information systems**
  - **Information security: encryption, virus scanners, firewalls, etc.**
  - **Also carry some cost**
    - ✓ installation, maintenance, computation time, lost ease-of-use, etc.
  - **Here too, dependent on…**
    - ✓ …risk of security breach
    - ✓ …potential damage in case of breach

- **Why Information Security?**
  - **Note**
    - **The risk of threats against information security is MUCH greater than the risk of threats against material objects**
      - ✓ Much more diverse attacks because of available computation power and almost ubiquitous network connectivity

Overview

- Security in the media
- Recent major incidents
- Why do we need security?
- Scope of the course

Scope of the course

- Chapter 1: Introduction
- Chapter 2: Basic concepts
- Chapter 3: Network and communication security
- Chapter 4: Software and systems security
- Chapter 5: Information security
- Chapter 6: Encryption algorithms
- Chapter 7: Legal aspects
- Chapter 8: Security Threads

Questions?

Besides the lecturers' own material, many third party, often copyrighted, material is reused within this lecture (e.g. in the notes) under the 'fair use' approach, for sake of educational purpose only, and very limited edition. As a consequence, the current slide set presentation usage is restricted, and is falling under usual copyrights usage.

At the end of every lecture, appropriate references to used materials are included.

References

- This work contains content adapted from, amongst other, the following sources (in no particular order)
  - William Stallings, "Cryptography and Network Security, principles and practices", 6th (international) edition, Prentice Hall, 2010;
  - Matt Bishop, "Computer Security: Art and Science", Addison Wesley, Pearson Education, 2003, ISBN-13: 978-0-201-44099-7
  - Lecture slides: "Informatiebeveiliging", Universiteit Gent, Eric Laermans & Thom Dhaene
  - Wikipedia (additional note page descriptions)
  - Various (web) comics and news sites (references given throughout the slides)
  - https://crypto.stackexchange.com/