Segurança de Software

Ibéria Medeiros

Departamento de Informática

Faculdade de Ciências da Universidade de Lisboa

Instructor

- Lectures
  - ☞ Prof. Ibéria Medeiros (imedeiros@di.fc.ul.pt)
  - ☞ Lecture times:

    [T] - Tuesday, 16h30-18h30, room 6.2.44

    [TP] - Tuesday, 18h30-20h00, lab 1.3.12
  - ☞ Student contact hours:

    Wednesday, 14:30h-16:15h, office 6.3.25

Communication

- Web Page: http://moodle.ciencias.ulisboa.pt/
  - ☞ official and current information of the course

- News group:
  - ☞ available in moodle
  - ☞ to be used by students and instructors for posting and discussion about all aspects of general interest

- Electronic mail (e-mail):
  - ☞ *imedeiros@di.fc.ul.pt*
  - ☞ eventually, direct communication with the instructors

- Student contact hours

Topics for the Semester

- Concepts, security protection provided by a computer (hw+OS) – part I
- Vulnerabilities and how to avoid creating them – part II
- Techniques and tools to discover vulnerabilities– part III

Requirements

- Operating systems
- Programming languages: C, Java e PHP
  - ☞ at least one of these languages
  - ☞ projects typically are based on programs in these languages
  - ☞ the exam normally has some simple exercises in C
- SQL

Bibliography

- M. Correia, P. Sousa, Segurança Informática no Software, 2nd Edition, FCA editora, 2017

- *Other books and papers are and will be made available in course web site …*

Grading

- Main components of the evaluation:
  - 45% Projects (includes class evaluation and final discussion)
    - 10% : presentation and discussion of conference papers
    - 5% : reports on class assignments (lightly graded)
    - 30% : project
  - 55% Final exam

- Notes
  - There will be 1 project in the lab, covering the area of manual and automatic vulnerability discovery
  - Projects are done in groups of 2 or 3 students
  - Dates for the projects are available in the web site

All evaluation elements are required

Minimum grade of 10 for both components of the evaluation!!!

FUTURE

- For students that want to work in this area, for instance in the context of their thesis, please contact me at the end of the semester

- European and national projects
  - SEAL: Secure Programming for Web Applications
  - XIVT: Excellence in Variant Testing
  - DISIEM: Diversity enhancements for SIEMs

Motivation to Software Security

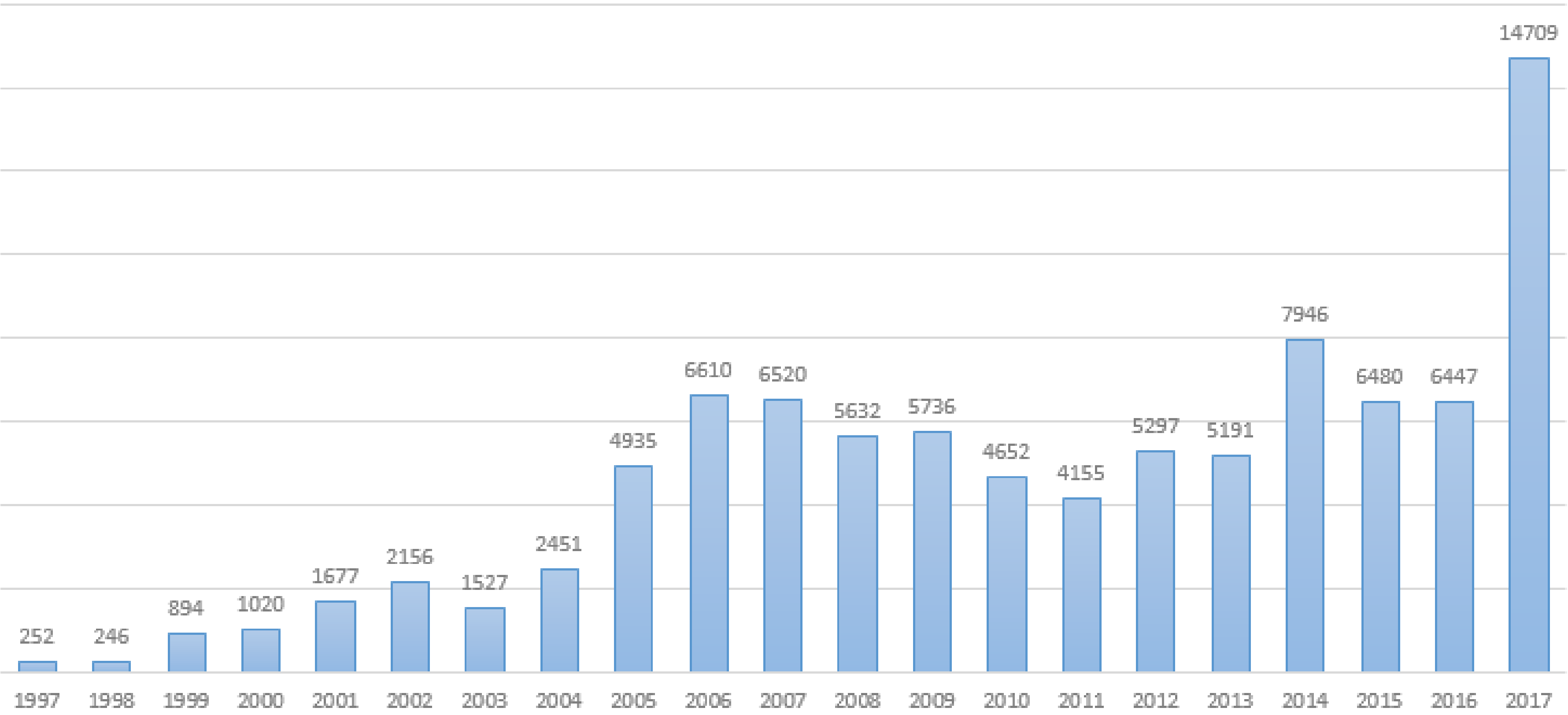
Ibéria Medeiros

Departamento de Informática

Faculdade de Ciências da Universidade de Lisboa

ONE OF OUR CUSTOMERS IS REPORTING SECURITY PROBLEMS WITH OUR SOFTWARE.
PREPOSTEROUS.
WHY?
BECAUSE OUR SOFTWARE DOESN'T *HAVE* ANY SECURITY?
OF *COURSE* IT DOES! LOOK AT THIS LOGIN SCREEN!
"ARE YOU A REGISTERED USER?
YES/NO"
Not Invented Here™ © Bill Barnes & Paul Southworth
NotInventedHere.com

Number of disclosed software vulnerabilities



10,644 vulnerabilities disclosed in the first half of 2018

Global Ransomware Damage Costs Predicted to Exceed $8 Billion in 2018 (Jun 2018)

Ransomware costs include damage and destruction (or loss) of data, downtime, lost productivity, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hostage data and systems, reputational harm, and employee training in direct response to the ransomware attacks.

Ransomware will attack a business every 14 seconds by the end of 2019

31TB of data were stolen - $3 Billion in US institutions (March 2018)

The Department of Justice indicted nine Iranian hackers over an alleged spree of attacks on more than 300 universities in the United States and abroad.

The attacks used carefully crafted spearphishing emails to trick professors and other university affiliates into clicking on malicious links and entering their network login credentials.

Of 100,000 accounts hackers targeted, they were able to gain credentials for about 8,000, with 3,768 of those at US institutions.

340 million records exposed
Rampant Data Exposures (2018)

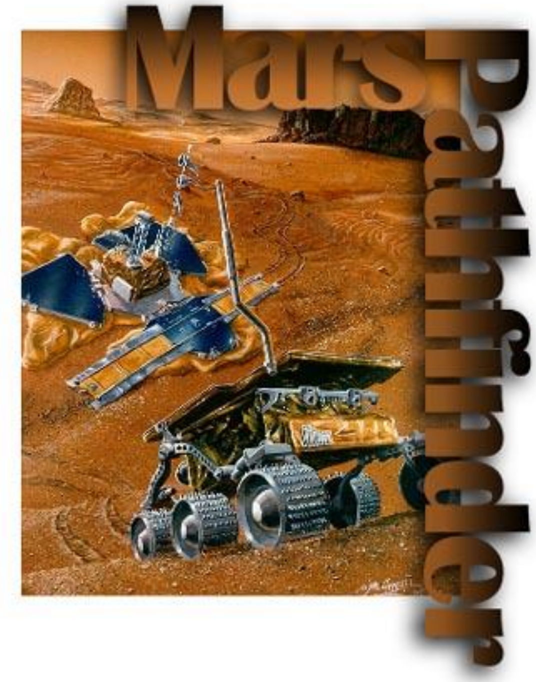
Data breaches have continued apace in 2018, but their quiet cousin, data exposure, has been prominent this year as well. A data exposure, as the name suggests, is when data is stored and defended improperly such that it is exposed on the open internet and could be easily accessed by anyone who comes across it. This often occurs when cloud users misconfigure a database or other storage mechanism so it requires minimal or no authentication to access. This was the case with the marketing and data aggregation firm Exactis. The trove didn't include Social Security numbers or credit card numbers, but it did comprise 2 terabytes of very personal information about hundreds of millions of US adults

Equifax Breach Affects Up to 143 Million (Sept 2017)

US credit bureau Equifax has acknowledged a breach that may have compromised as many as 143 million records. The exposed data include Social Security numbers (SSNs), birth dates, and driver's licenses. The breach also compromised payment card numbers of more than 200,000 consumers. Equifax detected the breach in late July and hired a forensics company to investigate the incident. The latest reports say that three Equifax senior executives sold nearly 1.8 million USD worth of company shares before the breach was publicly disclosed.

Bad SW is ubiquitous

- Airbus A400M military aircraft
  - ☞ Crashed due to the deletion of configuration files during a software update
- NASA Mars Lander
  - ☞ Crashed on Mars due to a units conversion bug ($165 million)
- NASA Mars Pathfinder
  - ☞ Stopped for several hours due to a priority-inversion bug ($265 million)
- Risks Forum: http://www.risks.org/



Bountie Hunters

- Offering a bug bounty is one of the best ways for software companies to find problems with their applications and services before they can be exploited.
- Offering a reward means those who find a flaw may opt to cash in, instead of selling it to those who would use it for nefarious purposes.
- Companies can offer tens, or even hundreds, of thousands for specific exploits, but it’s not easy money.

Bug bounty hunters must be an expert in all manner of security features and exploit mechanics

https://www.digitaltrends.com/computing/bug-bounty-hunters/

Bountie Hunters

- The US Air Force (USAF) launched a bug bounty program later 2017 spring (2017)

- USAF pays out $103,883 to hackers in bug bountie. 106 vulnerabilities found over a 20-day period. (February 2018)

- Intel expands bug bountie program, offers up to $250,000. Its maximum was $30,000 (February 2018)

I BROKE INTO THE WEB SITE TO *HELP YOU!*
THANKS, BUT IT'S *BETTER* IF WE DON'T KNOW THE SITE IS *INSECURE*.

When White Hat Hackers report discovered vulnerabilities, the outcome is not always what they expected.

White Hat Hackers

Security problems and more …

- US-CERT Technical Cyber Security Alerts
  - ☞ http://www.us-cert.gov/cas/techalerts/

- **TA18-201A :** Emotet Malware (banking Trojan)
- **TA18-149A** : HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm (malware used by the North Korean)
- **TA18-145A :** Cyber Actors Target Home and Office Routers and Networked Devices Worldwide (VPNFilter malware)
- **TA18-141A :** Side-Channel Vulnerability Variants 3a and 4 (Spectre and Meltdown)
- **TA18-106A :** Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices
- **TA18-086A :** Brute Force Attacks Conducted by Cyber Actors
- …

Example Use Case: Stuxnet

- *Malware for industrial control systems, probably those of “critical infrastructures” (power, gas, water,…)*
  - ☞ *Modifies programmable logic controllers (PLCs) that control these systems (weird but software too!)*
- *Some features:*
  - ☞ *Self-replicates through USB drives exploiting a vulnerability allowing auto-execution*
  - ☞ *Spreads in a LAN through a vulnerability in the Win.Print Spooler*
  - ☞ *Spreads through SMB by exploiting a Windows RPC vulnerabil.*
  - ☞ *Exploits another 2 unpatched privilege escalation vulnerabilities*
  - ☞ *Contains a Windows and a PLC rootkit*
  - ☞ *And many others…*

Source: Symantec W32.Stuxnet Dossier, Sep. 2010, version 1.0

Industry's fault?

Software buyers are literally crash test dummies for an industry that is remarkably insulated against liability, accountability, and responsibility for any harm, damages or loss that should occur because of manufacturing defects or weaknesses that allow cyber attackers to break into and hijack our computer systems.

☞ David Rice. “Geekonomics: The Real Cost of Insecure Software”,
Addison-Wesley, 2007

Schools' fault?

- “We at Oracle have (...) determined that most developers we hire have not been adequately trained in basic secure coding principles (…)
- We have therefore had to develop and roll out our own in-house security training program at significant time and expense. (...)
- In the future, Oracle plans to give hiring preference to students who have received such training and can demonstrate competence in software security principles.”
  - Mary Ann Davidson, Oracle’s Chief Security Officer

Trinity of trouble

1. Complexity
2. Extensibility
3. Connectivity

Other problems:

- time to market

Complexity

- Estimated 5-50 bugs per Klines of code
  - ☞ ~5 if rigorous quality assurance
  - ☞ Attacks exploit *bugs* called vulnerabilities
  - ☞ Examples:

– Solaris	7 M
– Netscape	17M
– Space Shuttle	10M
– Boeing	7 777M
– Windows 95	<5M
– Windows NT5	35M
– Windows XP	40M
– Windows Vista	50M
– MAC OS X 10.4	85M

Extensibility

- Current SW is inherently extensible:
  - Dynamic loadable device drivers, plugins, modules, DLLs,....
  - Virtual machines and mobile code (Java / .NET)
  - Combination of several components and forms of code execution (web apps)

- Problems:
  - What is “the software”? How do you ensure its security?

Connectivity

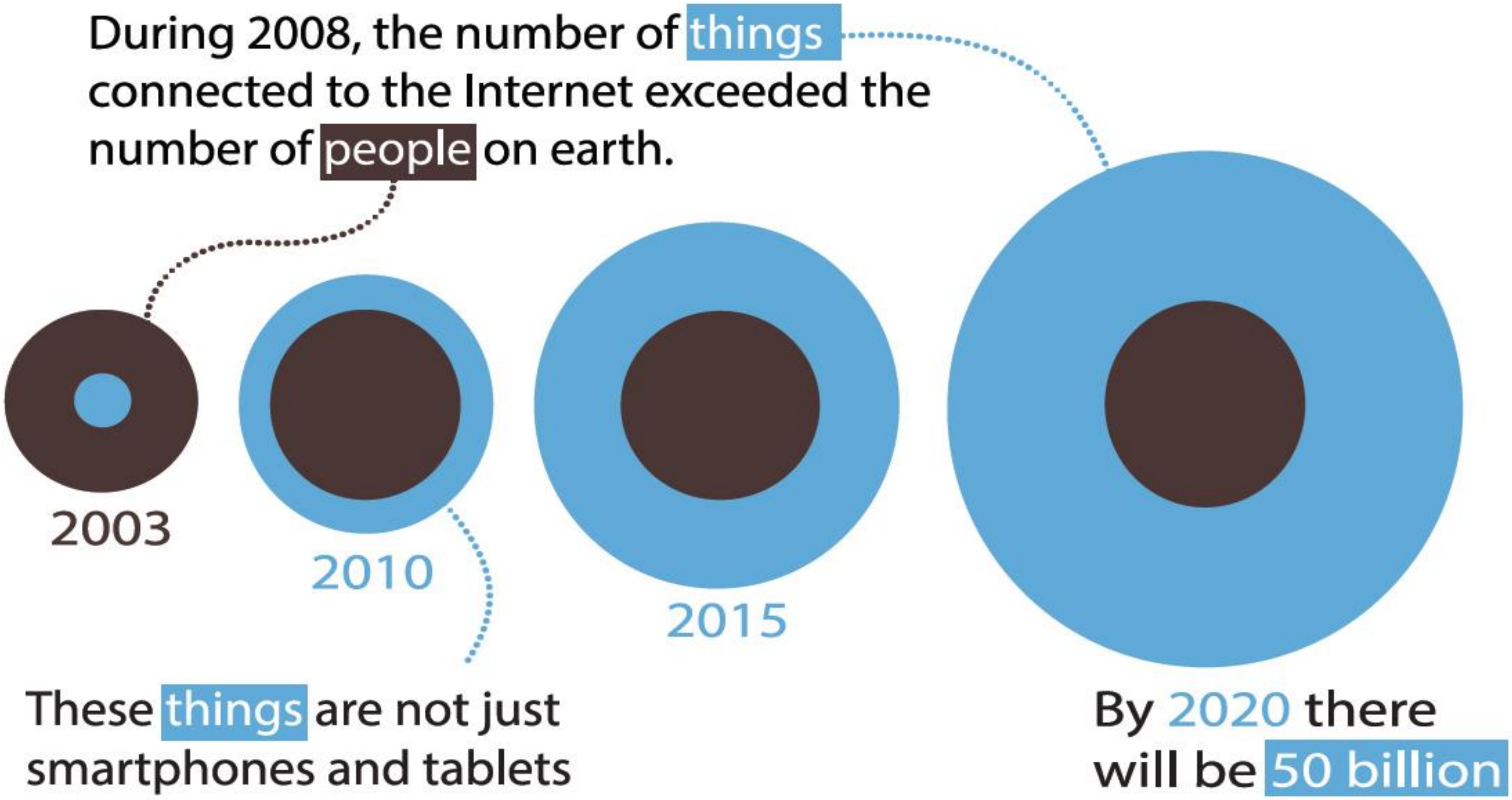
- Internet *(and mobile phones, PDAs,…)*
  - ☞ New bugs can propagate widely
  - ☞ Allows automated attacks
  - ☞ Agnostic to network solutions
    - SMS, email, IM, …
  - ☞ Economic risk
    - SWIFT net connects 7000+ banks and moves trillions of dollars daily
    - Hundreds of millions carry their smartphones, which are increasingly used to perform banking operations
  - ☞ Distance and feeling of safety; just a feeling …
    - international cooperation among polices has been making important arrests

(Near) future of SW

- More components
- More frameworks, more combination of binary and executed code
- More PDAs / smartphones
- More embedded systems (IoT)
- More wireless
- More distribution
- More mobile code
- Subscription services
- *More complexity, extensibility, connectivity*

Connectivity

Things connected to the Internet

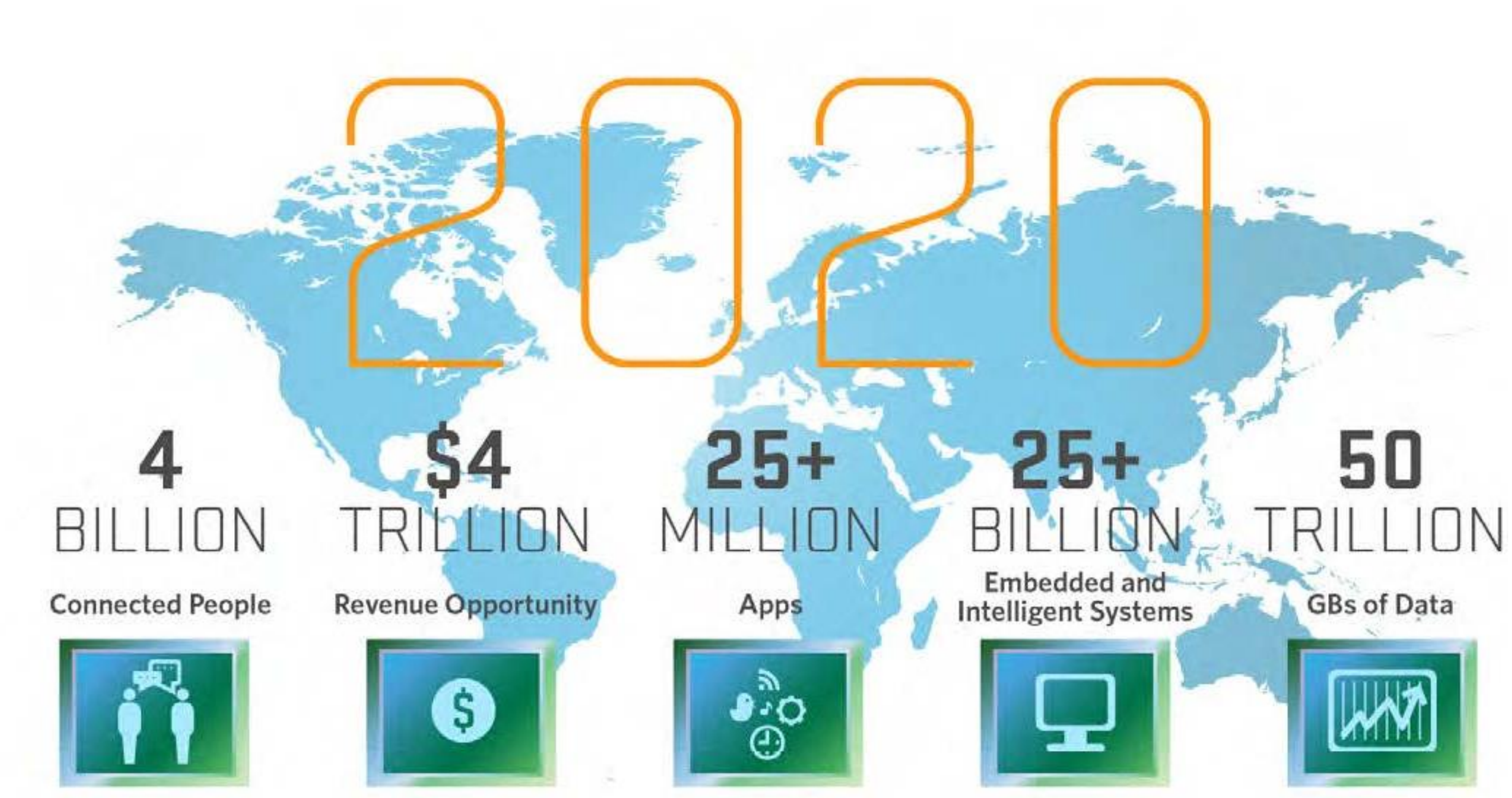


During 2008, the number of things connected to the Internet exceeded the number of people on earth.

These things are not just smartphones and tablets

By 2020 there will be 50 billion

Connectivity



Bibliography

- M. Correia, P. Sousa, Segurança no Software, FCA Editora, 2017 (see Introdução chapter)