Powered by

SECURITY MADEIN.LU

telindus

Hosted by

CYBERSECURITY BREAKFAST

TUESDAY SEPTEMBER 27TH, 2016

Namur, 2 Rue de Bitbourg,
1273 Luxembourg

From 8.15 am until 10.30 am

9th

**"Why is security not applied by default?
Do security-by-design!"**

scademy
secure coding academy

telindus

Secure coding

Do It Right at First

Telindus, Luxemburg
September 27, 2016

Gauthier Befahy

Essential security
for all software engineers.

IT security and secure coding

Essential security
for all software engineers.

Can you tell the difference between **security** and **safety**?

- Security timeline
  - Being secure **now** means that
  - based on **past** statistics we expect that in the **future**
    - probability of unwanted incidences will be small
    - and/or the caused damage will be small

Positive notions

Protection

Feeling secure

Confidential

Trust

Predictable

Reliability

Negative notions

Threat

Defenseless

Fear

Danger

Assumed security

Untrustworthiness

Attack

Unreliable

Exposed

Loss

Damage

Risk

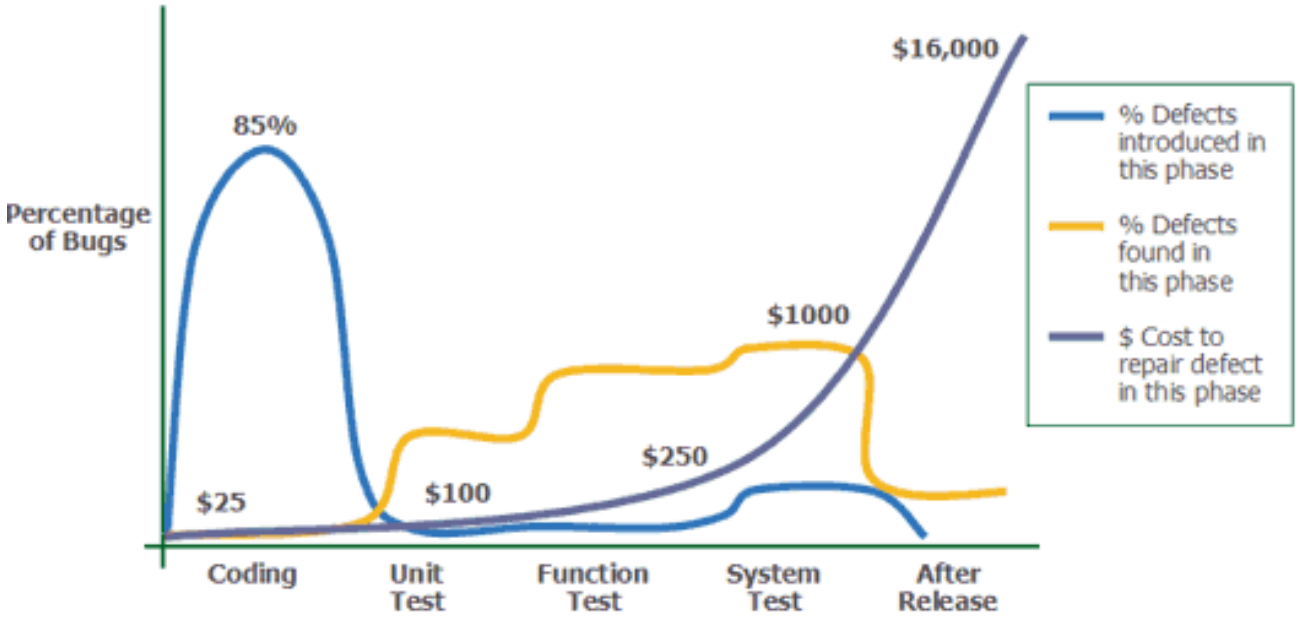
SDLC, Testing, and its Cost

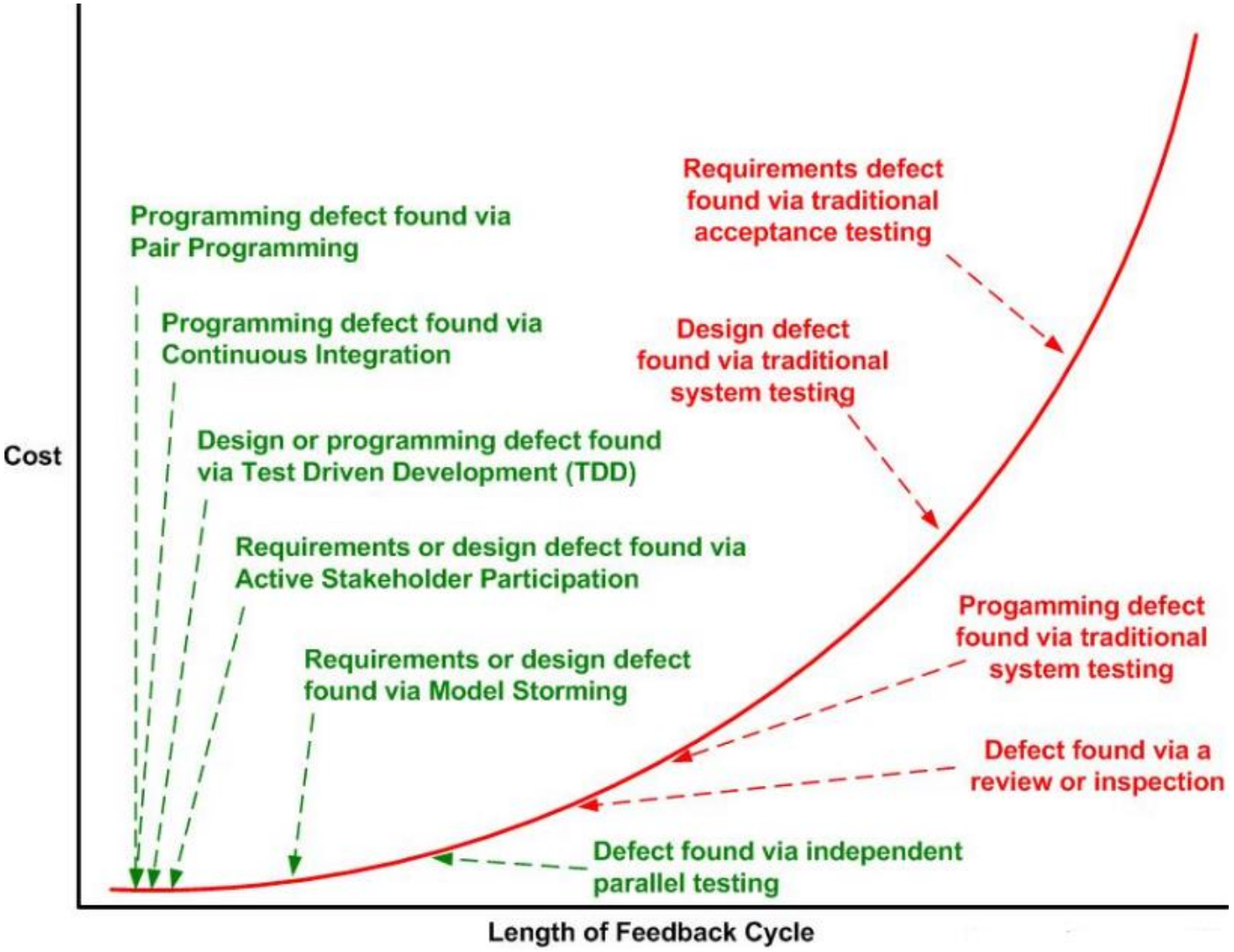
What is SDLC?

- It is a conceptual model used in project management that describes the stages involved in an information system development project.

Percentage of bugs per phase and costs to fix

Case Study




Cost
Length of Feedback Cycle
Programming defect found via Pair Programming
Programming defect found via Continuous Integration
Design or programming defect found via Test Driven Development (TDD)
Requirements or design defect found via Active Stakeholder Participation
Requirements or design defect found via Model Storming
Defect found via independent parallel testing
Defect found via a review or inspection
Progamming defect found via traditional system testing
Design defect found via traditional system testing
Requirements defect found via traditional acceptance testing

From vulnerabilities to botnets and cybercrime

Security flaws did exist, do exist and will exist...

- Cannot be fully avoided (cannot ever be 100% sure)
  - Seems to be an eternal cat-and-mouse game
  - So is it worth investing a lot of effort in a useless fight?
- To guarantee full protection is indeed very hard
  - And needs remarkable investments
  - But doing it right in the first place is "free"
    (90% of incidents stem from known problems!)
  - In addition, effective, cheap and specific protections do exist against **typical** security flaws
- Nevertheless the current situation is catastrophic
  - It is like driving cars at high speed without
    safety belts fastened...

- 1st reason: It is an unbalanced fight

  Available time and resources of the developers vs. motivation and preparedness of hackers

- 2nd reason: Security testing is challenging

  Functional testing checks for how the system should work, while in case of security it is about how the system should not work

- 3rd reason: Weak business motivation by market forces

  Due to the technical difficulties of measuring the level of security, there is no real customer enforced competition

- 4th reason: End-users suffer from the damage

  Developers are not motivated enough financially

- An average end-user may say: "*I do not store any valuable data on my computer, so why should I care?*"
  - Well, they should: effects emerge at a global level today

- Attackers' aims: world-wide spread of malware
  - Direct malicious intent: spyware, adware, ransomware, …
  - Build **botnets** – networks of zombie machines that they control
    - That are tools to commit wide-scale or targeted attacks (SPAM → phishing, cracking cryptography, DDoS, …)

- This is not done for fun any more
  - They make good money: **cybercrime** is a big business!
  - Even worse: attacking critical infrastructure
    - **Cyber war** and cyber terrorism are also emerging…

2014/2015 in Numbers

Cyber Breaches Hit Staggering Levels

Exceptionally harmful hacks have recently struck organizations in the global insurance, finance, telecom, and entertainment industries and at the heart of a U.S. federal agency—inflicting hundreds of millions of dollars in damage and added costs.

		How They Were Exploited	Data Stolen and Scale	Costs	Suspected Culprit
7/2014	**JPMORGAN CHASE** New York City	Two-factor authentication upgrade not fully implemented.	Names, addresses, and phone numbers of 76 million household and seven million small-business accounts.	The company says it plans to spend $250 million annually on security.	Three people have been charged with the attack as part of a stock manipulation scheme.
11/2014	**SONY PICTURES ENTERTAINMENT** Culver City, California	Malware and lack of intrusion detection.	E-mails, salary information, and terabytes of other data, including movie scripts and contracts.	$41 million, according to public filings.	North Korean regime.
2/2015	**ANTHEM HEALTH** Indianapolis	Malware specifically designed to attack the company.	Names, birth dates, addresses, employment information, and Social Security numbers for 78 million people.	Much or all of the $100 million value of its cyberinsurance policy.	China-based hackers, suspected to be affiliated with the government.
6/2015	**U.S. OFFICE OF PERSONNEL MANAGEMENT** Washington, D.C.	Likely social-engineering attacks and lack of modern intrusion detection services.	A mix of names, birth dates, addresses, fingerprints, and background information on as many as 21.5 million people.	More than $133 million just for credit monitoring for victims.	China-based hackers, suspected to be affiliated with the government.
7/2015	**ASHLEY MADISON** Toronto	Unknown, but attackers cited weak passwords and almost nonexistent internal security.	Names, addresses, birth dates, phone numbers, and credit card history of 37 million users, plus the CEO's e-mails.	Unknown. The company faces numerous lawsuits.	A previously unknown group that calls itself Impact Team.
9/2015	**T-MOBILE US** Bellevue, Washington	Security weaknesses at a partner (Experian) that was managing credit check data.	Names, birth dates, addresses, and Social Security and driver's license numbers of 15 million people.	Experian has spent at least $20 million on credit monitoring and other corrective actions.	Unknown.
10/2015	**TALKTALK TELECOM** London	Distributed-denial-of-service attack and malicious code.	Names, birth dates, addresses, and phone numbers of more than 150,000 customers.	About $50 million in lost sales and incident response costs.	A teenager in Northern Ireland.

Biggest Data breaches in 2016 (so far…)

- Anthem (second largest Health insurer in the USA)
  - 80 millions accounts were leaked (Names, dates of birth, social security numbers, adresses, employment information,…)
- Minecraft (Lifeboat Community)
  - 7 millions accounts were hacked (email adresses and passwords)
- Telegram
  - 15 million users' phone number were revealed by a group called „Rocket Kitten" from Iran.
  - Telegram was supposed to be **HIGHLY** secure.
- Others
  - Clinton Campaign, Mail.ru, Adult Friend Finder, Experian, Verizon, MySpace (same hacker as LinkedIn)

scademy
secure coding academy

Secure coding

Thank you!

Gauthier Befahy

gauthier.befahy@scademy.com

www.scademy.com

Join the **Secure Coding Academy** group on LinkedIn and stay informed about our courses!

Essential security
for all software engineers.