Robustness and Security Testing in SOA

Challenges & Opportunities

Marco Vieira
mvieira@dei.uc.pt
University of Coimbra – Portugal

IFIP WG10.4

Outline

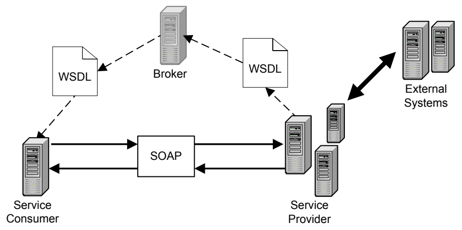
- The SOA trend…
- Robustness and security testing in Web Services
- Are Web Services robust and/or secure?
- Is it done? No, there are many challenges!

The SOA trend…

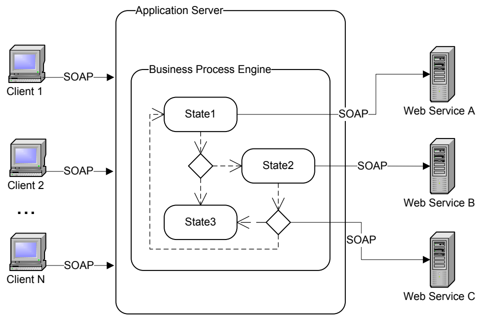
- Service Oriented Architectures (SOA)
  - Among the most important trends in modern software development
- Architectural style
  - Heterogeneous applications that exchange data
- Functionality decomposed into units (services)
  - Distributed over a network
- Supports business processes
  - Loosely coupled to their underlying implementations
- Support business- and mission-critical apps

Web Services

- Key support for SOA
- Provide a simple interface between a provider and a consumer

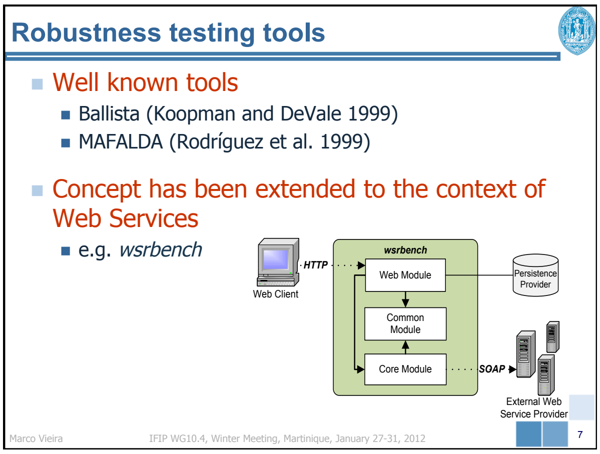


Web Services composition



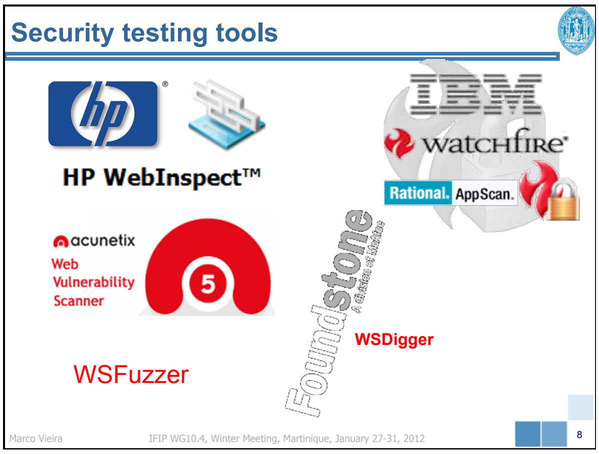
Robustness and security testing

- Well known concepts!!!
  - But, are they being applied in the WS context?
- Robustness Testing
  - Test a system/component focusing on limit conditions and invalid (out-of-domain) inputs
  - Looks for input validation problems
- Security (penetration) Testing
  - Submit malicious inputs to the service under testing
    - Inputs may be valid in the input domain
  - Looks for input values used in such way that may create security problems



Robustness testing tools

- Well known tools
  - Ballista (Koopman and DeVale 1999)
  - MAFALDA (Rodríguez et al. 1999)
- Concept has been extended to the context of Web Services
  - e.g. *wsrbench*



Security testing tools

HP WebInspect™

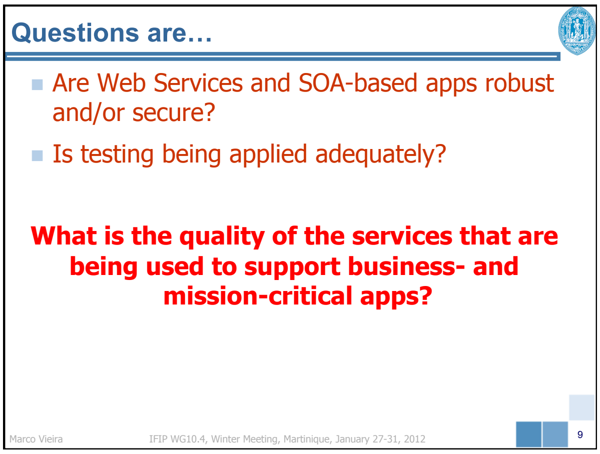
acunetix Web Vulnerability Scanner

WSFuzzer

Foundstone

WSDigger

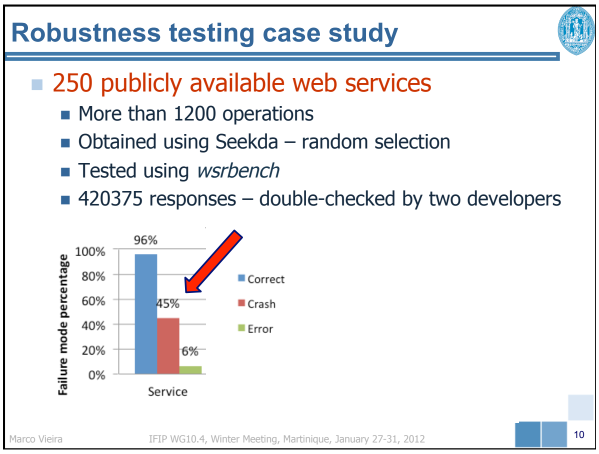
IBM watchfire Rational. AppScan.



Questions are…

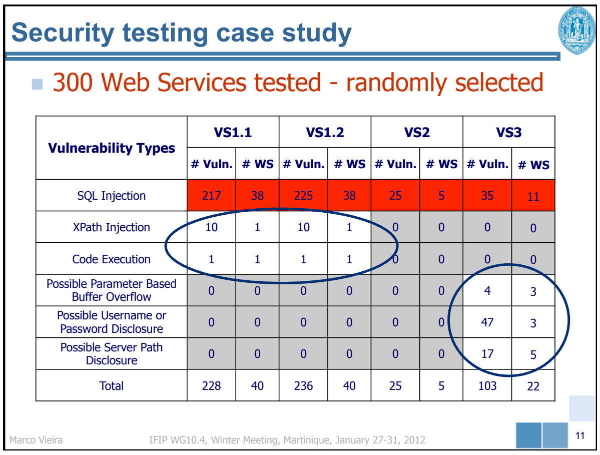
- Are Web Services and SOA-based apps robust and/or secure?
- Is testing being applied adequately?

What is the quality of the services that are being used to support business- and mission-critical apps?



Robustness testing case study

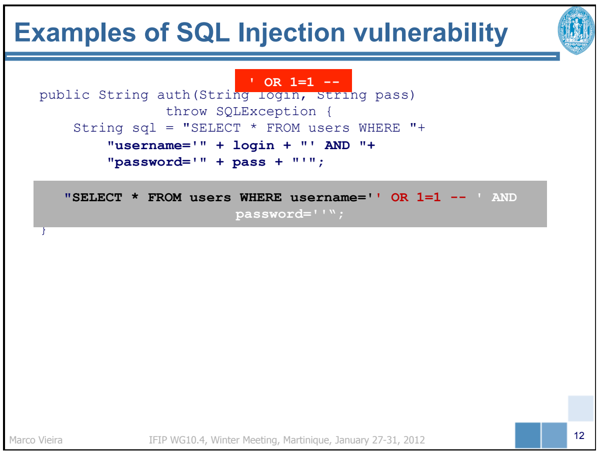
- 250 publicly available web services
  - More than 1200 operations
  - Obtained using Seekda – random selection
  - Tested using *wsrbench*
  - 420375 responses – double-checked by two developers



Security testing case study

- 300 Web Services tested - randomly selected

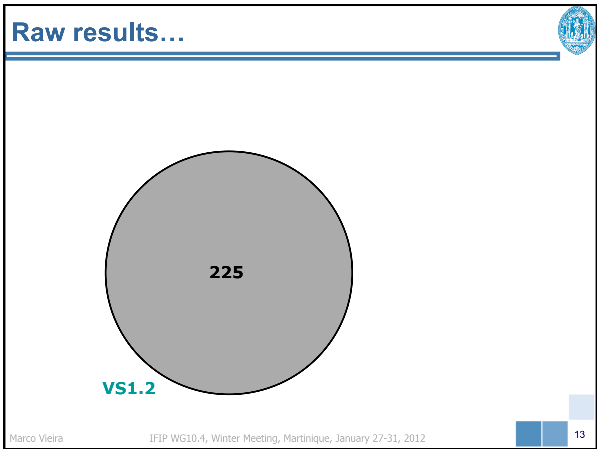
Vulnerability Types	VS1.1		VS1.2		VS2		VS3	
	# Vuln.	# WS	# Vuln.	# WS	# Vuln.	# WS	# Vuln.	# WS
SQL Injection	217	38	225	38	25	5	35	11
XPath Injection	10	1	10	1	0	0	0	0
Code Execution	1	1	1	1	0	0	0	0
Possible Parameter Based Buffer Overflow	0	0	0	0	0	0	4	3
Possible Username or Password Disclosure	0	0	0	0	0	0	47	3
Possible Server Path Disclosure	0	0	0	0	0	0	17	5
Total	228	40	236	40	25	5	103	22



Examples of SQL Injection vulnerability

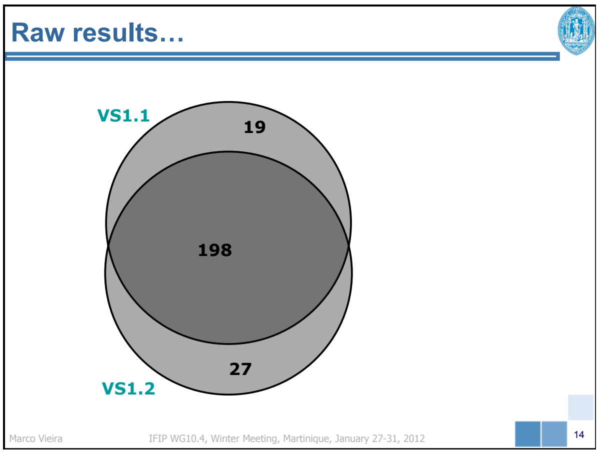
```
' OR 1=1 --
public String auth(String login, String pass)
               throw SQLException {
    String sql = "SELECT * FROM users WHERE "+
        "username='" + login + "' AND "+
        "password='" + pass + "'";

"SELECT * FROM users WHERE username='' OR 1=1 -- ' AND
                   password=''";
}
```



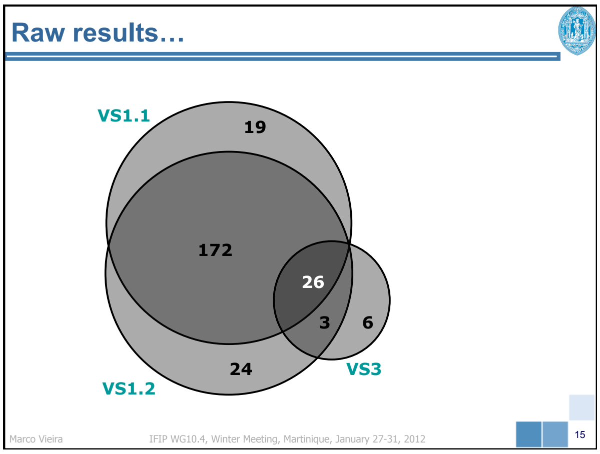
Raw results…

Marco Vieira IFIP WG10.4, Winter Meeting, Martinique, January 27-31, 2012 13



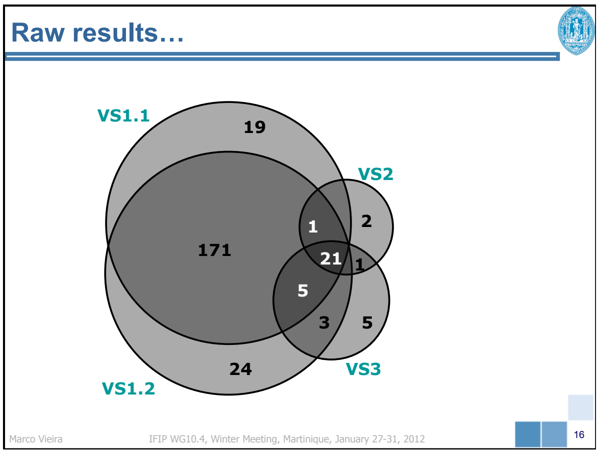
Raw results…

Marco Vieira IFIP WG10.4, Winter Meeting, Martinique, January 27-31, 2012 14



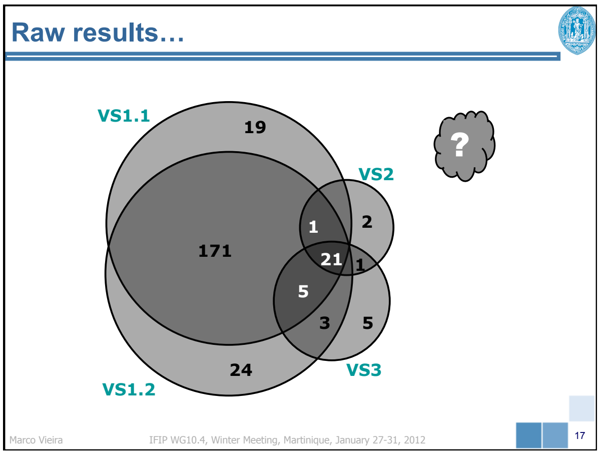
Raw results…

Marco Vieira IFIP WG10.4, Winter Meeting, Martinique, January 27-31, 2012 15



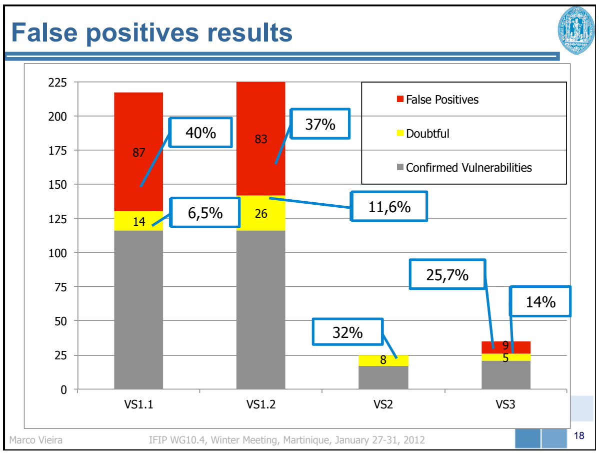
Raw results…

Marco Vieira IFIP WG10.4, Winter Meeting, Martinique, January 27-31, 2012 16



Raw results…

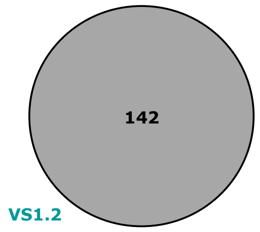
Marco Vieira IFIP WG10.4, Winter Meeting, Martinique, January 27-31, 2012 17



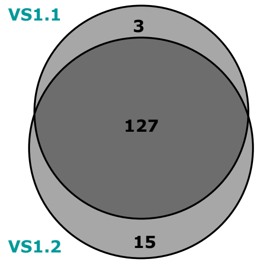
False positives results

Marco Vieira IFIP WG10.4, Winter Meeting, Martinique, January 27-31, 2012 18

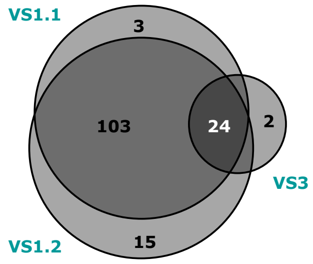
SQL Injection without False Positives



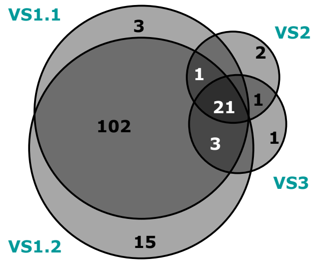
SQL Injection without False Positives



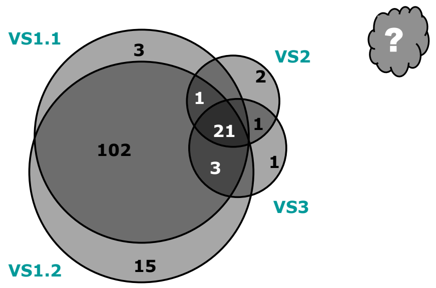
SQL Injection without False Positives



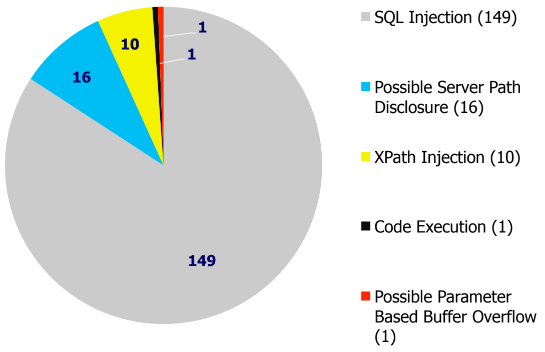
SQL Injection without False Positives

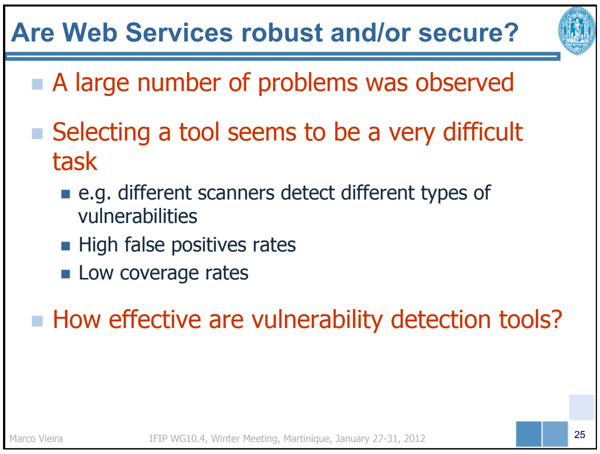


SQL Injection without False Positives



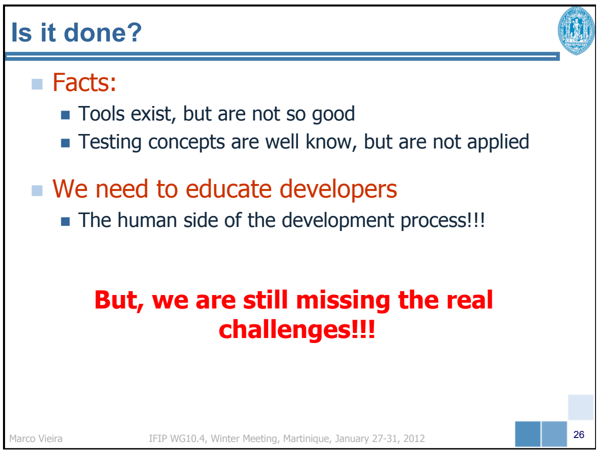
Common vulnerabilities





Are Web Services robust and/or secure?

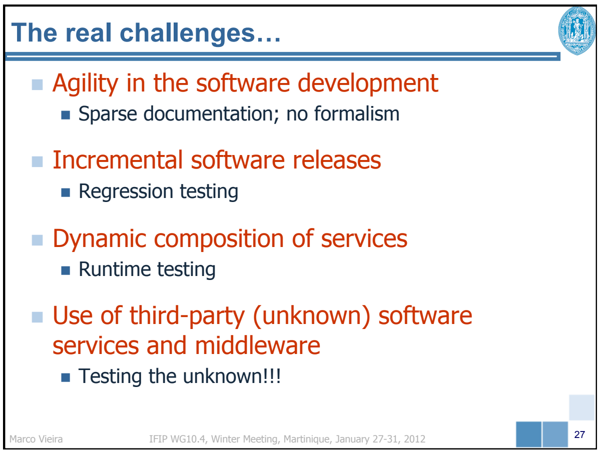
- A large number of problems was observed
- Selecting a tool seems to be a very difficult task
  - e.g. different scanners detect different types of vulnerabilities
  - High false positives rates
  - Low coverage rates
- How effective are vulnerability detection tools?



Is it done?

- Facts:
  - Tools exist, but are not so good
  - Testing concepts are well know, but are not applied
- We need to educate developers
  - The human side of the development process!!!

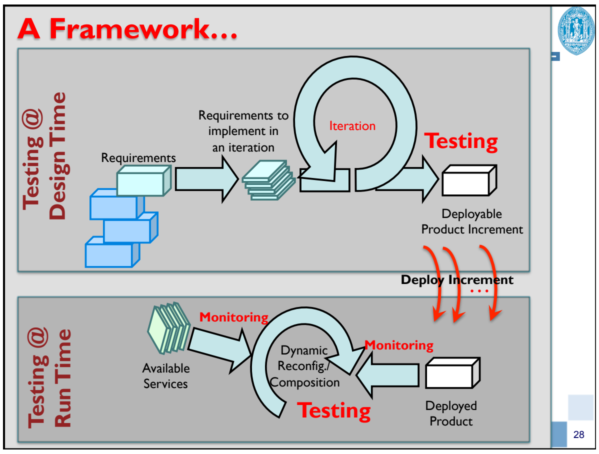
But, we are still missing the real challenges!!!

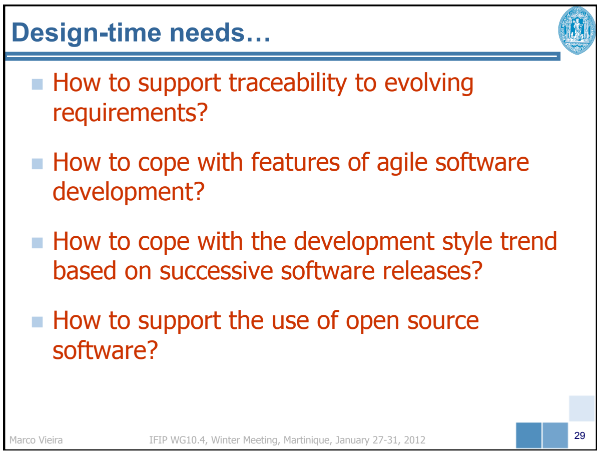


The real challenges…

- Agility in the software development
  - Sparse documentation; no formalism
- Incremental software releases
  - Regression testing
- Dynamic composition of services
  - Runtime testing
- Use of third-party (unknown) software services and middleware
  - Testing the unknown!!!

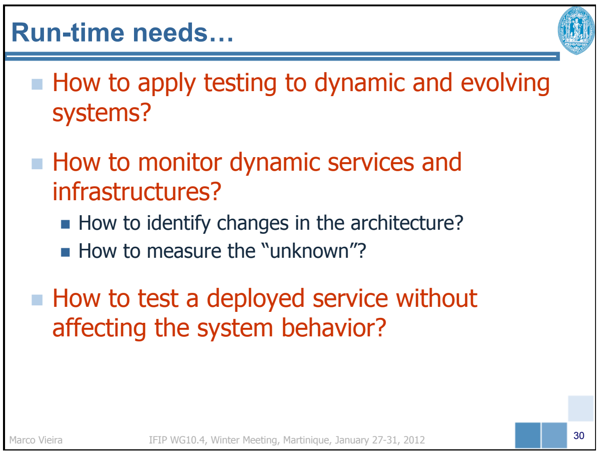
A Framework…





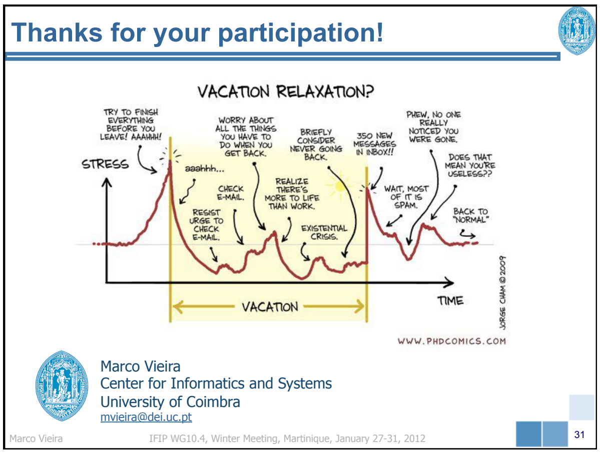
Design-time needs…

- How to support traceability to evolving requirements?
- How to cope with features of agile software development?
- How to cope with the development style trend based on successive software releases?
- How to support the use of open source software?



Run-time needs…

- How to apply testing to dynamic and evolving systems?
- How to monitor dynamic services and infrastructures?
  - How to identify changes in the architecture?
  - How to measure the "unknown"?
- How to test a deployed service without affecting the system behavior?



Thanks for your participation!

VACATION RELAXATION?
STRESS
TIME
VACATION
TRY TO FINISH EVERYTHING BEFORE YOU LEAVE! AAAHHH!
aaahhh...
RESIST URGE TO CHECK E-MAIL.
CHECK E-MAIL.
WORRY ABOUT ALL THE THINGS YOU HAVE TO DO WHEN YOU GET BACK.
REALIZE THERE'S MORE TO LIFE THAN WORK.
EXISTENTIAL CRISIS.
BRIEFLY CONSIDER NEVER GOING BACK.
350 NEW MESSAGES IN INBOX!!
WAIT, MOST OF IT IS SPAM.
PHEW, NO ONE REALLY NOTICED YOU WERE GONE.
DOES THAT MEAN YOU'RE USELESS??
BACK TO "NORMAL"
JORGE CHAM © 2009
WWW.PHDCOMICS.COM

Marco Vieira
Center for Informatics and Systems
University of Coimbra
mvieira@dei.uc.pt