RICECONSULTING

tsg Training

Welcome
Security Testing Webinar

Bernard Melson & Randall (Randy) Rice

September 20th, 2018

Today…


TSG TRAINING PRESENTS
ISTQB ADVANCED SECURITY TESTER WEBINAR
20-09-2018 | 13:00 BST
Security of our systems is a real big deal for us all, but how to test they are secure is a bit of a problem.
As a world leading expert in security testing, I'm absolutely delighted to welcome Randy to lead this webinar
tsg Training
Bernard Melson, MD
Randy Rice, Security Testing Expert

Agenda

- Security Testing – The challenges we face today
- The skills needed to test
- ISTQB Advanced Security
- Q&A
- Next Steps

Why Do the Security Breaches Continue to Occur?

- Human lapses
- Malicious insiders
- Malicious outsiders
- Lack of adequate defenses and testing of the defenses that *are* in place
- Defective software in general
- A limited view of security and testing
- Placing too much trust in technology
- Security is an afterthought in most development projects
- Lack of awareness at the executive level
  - Everybody knows cybersecurity is a problem, but very few people know how to deal with the risks and challenges.

DEFECT DAMAGES AND RECOVERY COSTS

Defect Origins	
1. Security defects	$200,000,000
2. Design defects	$175,000,000
3. Requirements defects	$150,000,000
4. Data defects	$125,000,000
5. Code defects	$100,000,000
6. Structural defects	$95,000,000
7. Requirements creep defects	$90,000,000
8. Web site defects	$80,000,000
9. Architecture defects	$80,000,000
10. Bad fix defects	$60,000,000
11. Test case defects	$50,000,000
12. Document Defects	$25,000,000
AVERAGES	$102,500,000

Defect recovery costs for major applications in large companies and government agencies

Copyright © 2011 by Capers Jones. All Rights Reserved.

Most organizations do not know the true status and strength of their information security defenses because they have never actually tested them!

Most organizations have a very limited approach to security testing, which mainly consists of penetration testing.

Many security vulnerabilities could be identified and eliminated if a wider, more robust view of security testing were promoted and performed.

However, security testing is a specialized activity and requires an extended level of knowledge beyond functional software testing. Specialized training is needed.

The Checklist

Correctly applied and working effectively?

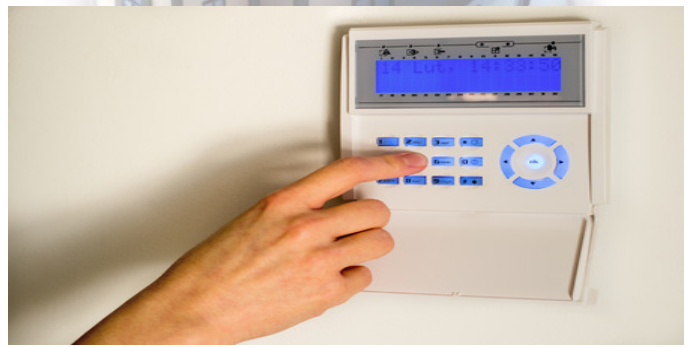
- Firewall installed? ☑ ?
- Intrusion detection installed? ☑ ?
- Encryption applied? ☑ ?
- Internal controls in place? ☑ ?
- Security policies and procedures defined? ☑ ?
- Physical security in place? ☑ ?
- Authentication and authorization applied? ☑ ?

tsg Training

RICECONSULTING

Think About Your Home Security

- Would you feel safe if…
  - You only checked the doors were locked once a month?
  - You had an alarm system but never actually heard the alarm sound?
  - You had alarm monitoring but had never been called by the monitoring company when the alarm is tripped?
  - You had no personal protection plan?



Yet, This is How Many People Think About Security Testing.

The Typical IT Security View of Security Testing

- Generally, limited to penetration testing
  - Perhaps also “bug bounties” and incident response testing
- Very little mention of functional security testing.
- This leaves many aspects of information security untested.

About the ISTQB Advanced Security Tester Certification

- In 2016, the International Software Testing Qualifications Board released the Advanced Security Tester Syllabus.
  - Written by 5 key authors from the USA and Europe.
  - Reviewed by over 20 ISTQB reviewers with security knowledge from both industry and government sectors worldwide.
  - References NIST guides and the NIST CSF heavily.

Advanced Security Tester Syllabus Outline

tsg Training

1. The Basis of Security Testing
2. Security Testing Purposes, Goals and Strategies
3. Security Testing Processes
4. Security Testing Throughout the Software Lifecycle
5. Testing Security Mechanisms
6. Human Factors in Security Testing
7. Security Test Evaluation and Reporting
8. Security Testing Tools
9. Standards and Industry Trends

https://www.istqb.org/downloads/send/46-advanced-level-security-tester/194-advanced-security-tester-syllabus-ga-2016.html

Our Goals in the Syllabus

tsg Training

- Have a lifecycle view of security and security testing.
  - “built in, not patched in”
- Be more than penetration testing.
  - Pen testing is very important, but limited.
- Everyone can have a role in security testing with the proper training and authorization.
- Give people (especially testers) a specialized career path.
- Contribute part of the solution to the huge cyber security challenges.

Where to Find the Syllabi

- All ISTQB Syllabi and sample exams can be freely downloaded from the ISTQB web site – https://www.istqb.org
  - Look in the “Downloads” section.
  - https://www.istqb.org/downloads/send/46-advanced-level-security-tester/194-advanced-security-tester-syllabus-ga-2016.html

Any Questions?

tsg Training

RICECONSULTING

Wrap-up

Many thanks to Randy for his experience and inciteful views.

Randy will be coming to TSG Training on November 12-15 to present an ISTQB Advanced Security Course. If you want to come along then:

- Mail: p.jones@tsg-training.co.uk
- Call: +44 20 3946 2720
- Web: www.tsg-training.co.uk/schedule
- Webinar: Say 'I'm interested the 'chat' box and we'll follow-up

This webinar will be posted on TSG Training's website and YouTube

Thanks for attending – we hope you found the webinar useful and will join us soon at TSG Training.