Training and Certifying Security Testers Beyond Penetration Testing

Randall W. Rice, CTAL (Full), CTAL-SEC
Director, ASTQB Board of Directors
www.astqb.org
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

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Correctly Applied</th>
<th>Working Effectively</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall installed?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Intrusion detection installed?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Encryption applied?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Internal controls in place?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Security policies and procedures defined?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Physical security in place?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Authentication and authorization applied?</td>
<td>✓</td>
<td>?</td>
</tr>
</tbody>
</table>
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.
Penetration ("Pen") Testing

• Is needed and is helpful
• But...
  – It is a snapshot
  – Follows the "event" model and typically can’t be sustained
  – Lacks the internal view of security
There Are No Easy Answers

• There is no single solution.
• However, it is clear we can and must do better in safeguarding valuable physical and digital assets.
• It’s like Y2K without the deadline!
What is Needed?

• A holistic approach that involves software testers, with security testing as a priority in all project activities.
  – Continuous security testing in all forms
  – Testing perspectives from multiple roles
• Strong executive leadership.
  – Board presence or command presence is needed
  – Independence is needed
  – The CISO may not be independent enough for board-level accountability
• Complete organizational compliance and involvement
Security Testing is Not an Event.

It Should be a Continuous Activity.
Major Questions

• Who should perform security testing?
  – Internal testers?
  – Contractors?
  – Security admins?

• How are these testers trained and developed?
  – Classroom training – including hands-on experience
  – Certification in security testing techniques – beyond pen testing
  – Actual experience
  – Continued learning and awareness
Big Challenges for the U.S. Federal Government

“...in fiscal year 2015, 19 of the 24 major federal agencies covered by the Chief Financial Officers Act of 1990 reported that information security control deficiencies were either a material weakness or significant deficiency in internal controls over financial reporting. In addition, inspectors general at 22 of the 24 agencies cited information security as a major management challenge for their agency.”

Testimony Before the President's Commission on Enhancing National Cybersecurity – Sept. 19, 2016

Both Internal and External Views are Needed

- Application/System
- Organization
- Device/Product
MOVIE HACKING...

IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.

REAL HACKING...

HI, THIS IS ROBERT HACKERMAN. I’M THE COUNTY PASSWORD INSPECTOR.

HI BOB! HOW CAN I HELP YOU TODAY?
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.
The nature of software defects and security vulnerabilities.

The impact of defects (of any type) can migrate throughout an organization.

Trained and certified security testers should be able to design and perform tests to identify these defects and vulnerabilities.
Arguments Against Internal Security Testing

• “Our people don’t have the technical knowledge.”
• “Our people don’t understand security exploits.”
• “Our people don’t think like attackers.”
• “Our people haven’t been trained in security testing.”
• “We don’t want to expose sensitive data to functional testers.”
• “Security testing is too expensive.”
## WORK HOURS AND COSTS FOR DEFECT REPAIRS

<table>
<thead>
<tr>
<th>Defect Origins</th>
<th>Work Hours</th>
<th>Costs ($75 per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security defects</td>
<td>10.00</td>
<td>$750.00</td>
</tr>
<tr>
<td>2. Design defects</td>
<td>8.50</td>
<td>$637.50</td>
</tr>
<tr>
<td>3. Requirements creep defects</td>
<td>8.00</td>
<td>$600.00</td>
</tr>
<tr>
<td>4. Requirements defects</td>
<td>7.50</td>
<td>$562.50</td>
</tr>
<tr>
<td>5. Structural defects</td>
<td>7.25</td>
<td>$543.75</td>
</tr>
<tr>
<td>6. Architecture defects</td>
<td>7.00</td>
<td>$525.00</td>
</tr>
<tr>
<td>7. Data defects</td>
<td>6.50</td>
<td>$487.50</td>
</tr>
<tr>
<td>8. Bad fix defects</td>
<td>6.00</td>
<td>$450.00</td>
</tr>
<tr>
<td>9. Web site defects</td>
<td>5.50</td>
<td>$412.50</td>
</tr>
<tr>
<td>10. Invalid defects</td>
<td>4.75</td>
<td>$356.25</td>
</tr>
<tr>
<td>11. Test case defects</td>
<td>4.00</td>
<td>$300.00</td>
</tr>
<tr>
<td>12. Code defects</td>
<td>3.00</td>
<td>$225.00</td>
</tr>
<tr>
<td>13. Document defects</td>
<td>1.75</td>
<td>$131.50</td>
</tr>
<tr>
<td>14. Duplicate defects</td>
<td>1.00</td>
<td>$75.00</td>
</tr>
<tr>
<td><strong>AVERAGES</strong></td>
<td><strong>5.77</strong></td>
<td><strong>$432.69</strong></td>
</tr>
</tbody>
</table>

Maximum can be > 10 times greater
## 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.
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.
ISTQB and ASTQB

• ASTQB, the American Software Testing Qualifications Board, is the U.S. board for the internationally recognized ISTQB software testing certification.

• Our mission is to promote professionalism in Software Testing in the United States.

• Founded in 2003, the ASTQB has certified over 21,000 testers in the USA.
  – Our certificate holders come from all sectors – Finance, Defense, Manufacturing, Medical, Software Vendors and many others.
ISTQB

• ISTQB is the International Software Testing Qualifications Board.
• It is composed of representatives from each existing national board, such as the ASTQB.
• The ISTQB decides on the standards for certification and accreditation as an ISTQB accredited training provider.
• Working parties within ISTQB are responsible for developing and maintaining the various software testing syllabi and exams.
• As with ASTQB, all members are volunteers.
• Most of the ASTQB/ISTQB certifications are for life – no reaccreditation is needed.
  – New certification for expert levels have a 5-year period of validity.
3rd Largest Certification Program Worldwide

- As of December 2016, ISTQB® has administered over 700,000 exams and issued more than 500,000 certifications in over 117 countries world-wide.
  - 57 country boards at this time.

- The program relies on a Body of Knowledge (Syllabi and Glossary) and exam rules that are applied consistently all over the world, with exams and supporting material being available in many languages.
ASTQB Mission

• We do this by providing and administering quality exams for the ISTQB, ASTQB and IQBBA certifications, by supporting and facilitating training providers in delivering high quality courses, by actively engaging in the ISTQB working groups, and by supporting efforts to develop and encourage people who are already in or are entering the software testing profession.
Building Your Foundation
ISTQB and ASTQB certifications offer a road map to guide your career.

START HERE

ISTQB Certified Tester Foundation Level

RECOMMENDED FOR ALL CAREERS
Whether you are looking for a software testing job, or already have a job as a tester, this is where you need to start. The Certified Tester, Foundation Level (CTFL) is the gateway certification for all the other ISTQB certifications.

Advancing Your Career
Which of these best describes you?

I want to work with customers.
This certification is designed for the tester who has a deep understanding of the business domain and the needs of the user.

I want to work with code.
This certification is designed for the technically minded individual who wants to and is capable of programming, both in scripting languages (e.g., Python) as well as standard programming languages (e.g., Java).

I want to lead the team.
You will learn all about test planning, monitoring, and controlling for projects that you will also learn about delivering best strategies and plans that can change the course of testing for the organization.

I want to be part of an agile team.
This certification will enhance your vocabulary and teach you the best approach to testing on an agile project and will help you understand how you can be most effective in that environment.

I want to stand out.
Build your career with a combination of 4 business analysis processes.

I want to focus on agile.
You're ready to be a leader in the agile environment, and ISTQB Advanced Agile Testing gives you the knowledge and skills to be that leader.

I want to specialize.
Do you need knowledge 4.0.4.0, or high profile advanced testing?

Learn more at: www.astqb.org
Advanced Security Tester Syllabus Outline

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

Our Goals in the Syllabus

• 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 ASTQB web site – https://www.astqb.org
  – Look in the “Library” section.
Exam Details

• To take the ISTQB Advanced Security Tester exam, the candidate must:
  – Hold the ISTQB Foundation Level certification
    • Covers a wide range of testing practices
    • Costs $250
    • Training is not required, but encouraged
  – Have 3 or more years in the software testing field, or a related field, such as software development, security administration, business analysis, etc.
  – Pay an exam fee of $200
  – Training is not required but highly encouraged.
  – There are no discounted re-take provisions.
  – All ASTQB/ISTQB exams are covered by the GI Bill.

• All exams (except Expert levels) consist of multiple-choice questions.
Exam Details (2)

• All ASTQB/ISTQB exams can be taken electronically and there is e-learning available from training providers.
  – Exams are taken at Kryterion exam centers worldwide.
  – Paper exams are available for groups of 3 or more people.
    • Such as in the case of in-house classroom training.

• http://www.kryteriononline.com/ Locate-Test-Center
About Training

• Since the main objective is to educate people in how to plan, conduct and evaluate security testing, training is a key element.
  – The goal is to do much more than just pass an exam.
  – This is true for all of the ISTQB/ASTQB certifications.
  – However, all ISTQB exams can be taken without formal training.

• Training is available from training providers in the USA and other countries.
  – USA training providers are accredited by the ASTQB as a form of quality control.
Training Course Lengths

• ISTQB Foundation Level Course – 3 to 4 days
• ISTQB Advanced Security Tester Course – 3 to 4 days
• Times vary depending on the training provider and their approach.
Tangible Steps

• Raise awareness at all levels
  – Not just that “cybersecurity is important”
  – We are not doing nearly enough to stay even close to vigilant.
• Assess risks and threats continuously.
• Get training
  – The ISTQB Advanced Security Tester certification is a great start.
• Build your framework – soon.
  – You don’t have to start from scratch.
Resources

- ASTQB Web Site – https://www.astqb.org
- ISTQB Web Site – https://www.istqb.org
Your Questions?
Bio - Randall W. Rice, CTAL-SEC

- Over 35 years experience in building and testing information systems in a variety of industries and technical environments
- ISTQB Certified Tester – Foundation level (CTFL), Advanced Level (CTAL) Full, Advanced Security Tester (CTAL-SEC)
- ASTQB Certified Mobile Tester (CMT)
- ISTQB Foundation Level Agile Tester (CTFL-AT)
- Director, American Software Testing Qualification Board (ASTQB)
- Chairperson, 1995 - 2000 QAI’s annual software testing conference
- Principal Consultant and Trainer, Rice Consulting Services, Inc.
Contact Information

Randall W. Rice, CTAL (Full), CTAL-SEC
Ph: 405-691-8075
e-mail: rrice@astqb.org
LinkedIn -
https://www.linkedin.com/in/randallrice1/