A Different Mindset for Testing

Functionality versus Security

Presentation for Testnet members

Location provided by Equens Netherlands

GLOBAL CAPABILITY.
PERSONAL ACCOUNTABILITY.

Rein van Koten, CISA, CISSP, PCI-DSS QSA
Principal Consultant Information Security

August 27, 2009

PROPRIETARY STATEMENT

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

verizonbusiness

Introduction

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

Rein van Koten …. breaking stuff is just a habit…

Person
- Apparently started with security at the age of 3 ??
- Wrote first security report during high school ….
- Enjoys diving and making music.
- Does have a social life ☺

Job
- Joined Cybertrust July 2007.
- Principal Consultant Information Security.
- Managing Consultant for PCI-DSS in Benelux & Middle East.
- Lead for Dutch Penetration Testing Team.

Professional view on Information Security:
- Information Security is just an other part of Governance, Risk & Compliance.
- If it is not worth protecting, accept risk and be prepared to absorb loss.
- Most of it should already be common practice for a lot of other reasons….

Personal view on Information Security
- Nice, so what else can we do with it?
- Nice, but why?
- Now how does it do that?
- How are we going to do this in the future?

verizon business

Introduction Verizon Business Security Solutions

VzB Security Solutions is a combination of:

- » Cybertrust
- » Ubizen
- » TruSecure
- » Netsec
- » Entrust / Baltimore
- » ICSA labs

Covers anything from Managed Security Services, Security Operations, Vulnerability Assessments and Penetration Testing up to Governance, Risk, Compliance, Audits, Certifications, Forensics and Security Consulting.

Acknowledged World Leader in Information Risk Intelligence.

Part of Verizon Business and Verizon Communications

- »Global communications provider.
- »Hosting.
- »Virtualization.

Verizon Business and Cybertrust Join Forces

A Global Security Powerhouse

verizon business + cybertrust = verizon business

Security Solutions powered by Cybertrust

- Operating unit of Verizon Communications – ranked 13th in U.S. Fortune 500
- Advanced voice, data, IP, IT and wireless solutions for large business and governments
- One of the largest and most secure global IP networks serving 2,700 cities in 150 countries
- Manage networks and/or security for over 4,000 enterprises and government agencies around the world

- Global provider of managed security services
- 15+ years' experience securing critical data and protecting identities
- Professional services for threat, compliance/ vulnerability, and identity management
- First information security certification program (1997)
- ICSA Labs – most recognized provider of information security testing and certification

- Largest global provider of managed information security services
- Comprehensive solutions based on level of risk and risk tolerance
- Flexible service delivery – self-service, managed, hosted, and outsourced
- Increased visibility for fast and efficient mitigation actions
- Seven SOCs and over 1,100 security professionals worldwide

Managed security solutions for large businesses and governments

Agenda & Approach

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

Agenda

- Setup of this presentation
- History of this idea
- Focus on security testing increases
- Security testing in context
- Functional Testing versus Security Testing approach
- Where to go for more information
- Discussion

Presentation Setup

- **A lot information with very little technical detail.**
- **Not assuming security skills, although it does help.**
- **Aimed at people in charge of embedding security testing into software development lifecycle.**
- **Black and white statements to provoke thought.**
- **Hacker / Cracker / Curious Person / (ab)user; let's not go there.**
- **"Associative presentation", don't worry about the order of things.**

By the way:

  – I do not know much about testing methods….
  – I can talk about this for days, you have been warned!

History of this idea

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

It started with a discussion on secure application development requirements for PCI-DSS

THE QUESTION

…. so just tell me sir, what exactly testers need to test for this “SQL Injection” and we will include it in our test cases….

Au, Flash, Help!

How do you tell someone who is used to testing what something SHOULD do, that they should now test ALL OTHER scenarios as well ??

(… yes I know, this is not exactly correct)

I realized a change in mindset was necessary.

verizon business

Focus on security testing increases

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

Focus on security testing increases (1)

Sorry, I just can't skip this part but I'll be very brief

- **"Hackers" are "moving up the stack" as operating systems generally are getting hardened and patched. Focus is now more on application security.**
- **Processing environments get more complex. Think about mash-ups using many other parties' developments.**
- **Assumptions from the past no longer hold:**
  - This is internal only, it is not the internet. How about your service providers?
  - We only provide access to our own employees. How about your business partners?
  - Part of the stack is no longer under your own control. Hosting, ASP, Cloud.
- **And everyone's favorite: Compliance:**
  - Privacy Laws / Government regulation
  - Financial regulation (SOx, IFRS)
  - Industry regulation (PCI-DSS)
  - Liability and Accountability

verizon business

Focus on security testing increases (2)

PCI-DSS Requirement 6: Develop and maintain secure systems and applications

- **Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.**
- **Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.**

Source: PCI Secure Standards Council

verizon business

Focus on security testing increases (3)

6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. …..

- » Testing of all security patches, and system and software configuration changes before deployment, …
- » Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)
- » Validation of proper error handling
- » Validation of secure cryptographic storage
- » Validation of secure communications
- » Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability
- » …..

6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the *Open Web Application Security Project Guide.* Cover prevention of common coding vulnerabilities in software development processes, to include the following:

- » Cross-site scripting (XSS)
- » Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
- » Malicious file execution
- » Insecure direct object references
- » Cross-site request forgery (CSRF)
- » Information leakage and improper error handling
- » Broken authentication and session management
- » Insecure cryptographic storage
- » Insecure communications
- » Failure to restrict URL access
- » ...

Please note: this is just a partial selection of the requirements!

Source: PCI Secure Standards Council

verizonbusiness

Security testing in context

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

Security testing in context (1)

Some parts of the bigger picture surrounding security testing:

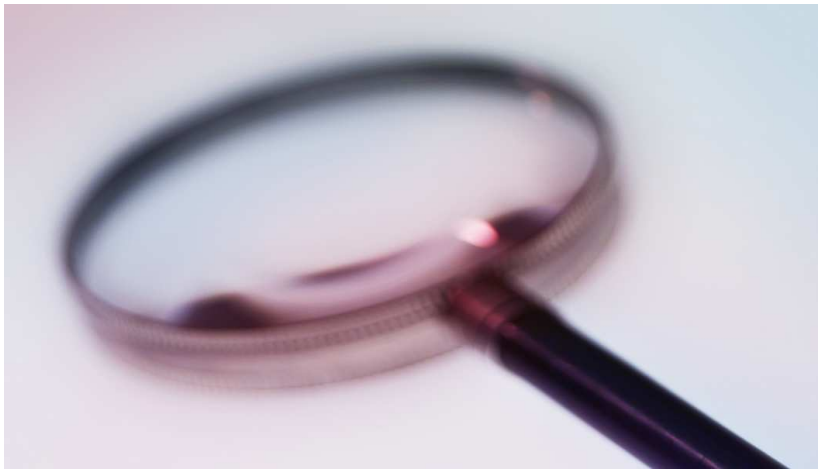
- **Business Impact Assessment, Threat & Vulnerability Assessment, Risk Assessment, Control Selection:**
  - Provides input for testing on effectiveness of selected mitigation strategy.
  - Testing subjects are defined, but not the exact test scenario's.
    - »Example: How do you test if chosen authorization mechanism is secure?

- **Secure coding practices to lower number of vulnerabilities:**
  - Prevention is always better than correction.
  - Everyone tells me this is much cheaper, so why is this so hard?

- **Security of development environment and tooling:**
  - Did you ever test the security of your development environment or processes?
  - Who has access to your code?
  - And how secure is your versioning solution (Clearcase, CVS, SVN etc)?
  - Compiler options?

Security testing in context (2)

- **Source code review**
  - Static code review.
  - Dynamic code review.
  - Manual review or tools.



- **Vulnerability Assessments**
  - Dedicated tools to identify known issues.
  - Penetration Testing.

- **Other techniques or processes that might be used**
  - Fuzzing.
  - Abuse Cases.

But this is not what we are going to talk about today! ☺

Functional Testing versus Security Testing approach

Some interesting differences

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

The Mindset Difference

A developer is concerned with what the application should do, a hacker thinks about what else he could make it do…

From a functional point of view, it is known what the application should do. Therefore testing of functionality in theory can be done for 100% of all possible uses.

Question: Should an application only do exactly what is in the functional specifications, and ABSOLUTELY NOTHING MORE?

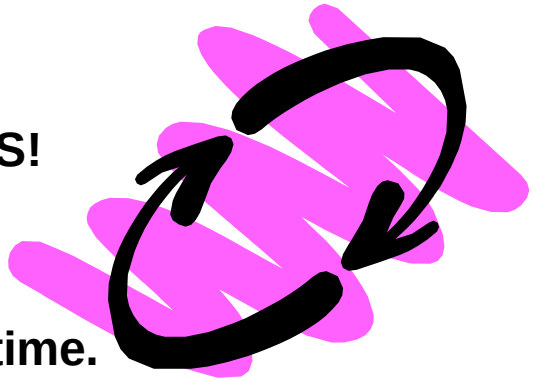
So what about insecure functional specifications?

verizon business

If everything passed the tests, we're done right? (1)

Question:

If you could completely test ALL functionality and intended uses and every thing is 100% OK, is there a need to repeat testing at regular intervals during the application lifetime?



From a security point of view the answer certainly is YES!

Some reasons:

- **New exploits in all components used are found all the time.**
- **The impossible becomes possible, e.g. because of increased bandwidth or computing power.**
- **Assumptions are proven wrong.**

Do you know the current security application of the Playstation 3?

Answer: Hundreds of them combined to form
super computer to attack passwords or encryption schemes!

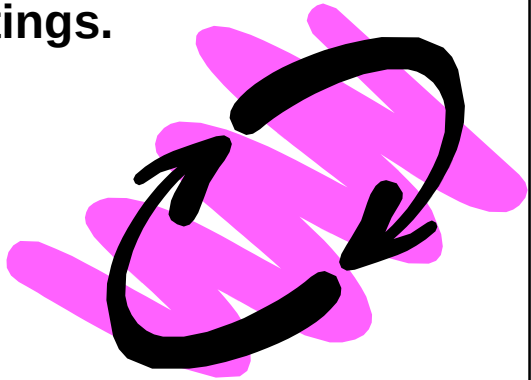
verizon business

If everything passed the tests, we're done right? (2)

And remember if you started with BIA, T&VA, RA and CS:

- **Assumptions on existing mitigating controls can be invalidated.**
- **New threats become known.**
- **Controls themselves develop weaknesses.**
- **Business Impact increases, therefore associated risk ratings.**

How much importance was assigned to security during initial design and development?



And security tools for code review & vulnerability assessment have new checks added daily. The bad guys also have these…

What is secure today is broken tomorrow

Example of a serious issue some time ago:

Your tool is a simple lightweight web server and it even checks for illegal things like ..\..

Everything works nicely and global computer vendors even use your web server in their monitoring tools and everyone is happy.

Then two years later along comes this irritating guy that is checking the security of a server with this tool on it.

As now it is known there are other ways to generate sequences that result in ..\.. he tries this and… uses this web server to completely compromise the server, the domain and the company… (certainly one of my better days)

If you or the computer vendor had checked the application regularly with current tools, the issue would have been identified much earlier…

New vulnerabilities in your tooling

Even if your own code would be completely secure all the time, other things in the environment might create unexpected vulnerabilities….

Several weaknesses were found in compilers that enforced buffer length checks incorrectly.

- »Do you know exactly what security options you use in your compiler settings?
- »And do you review these regularly?

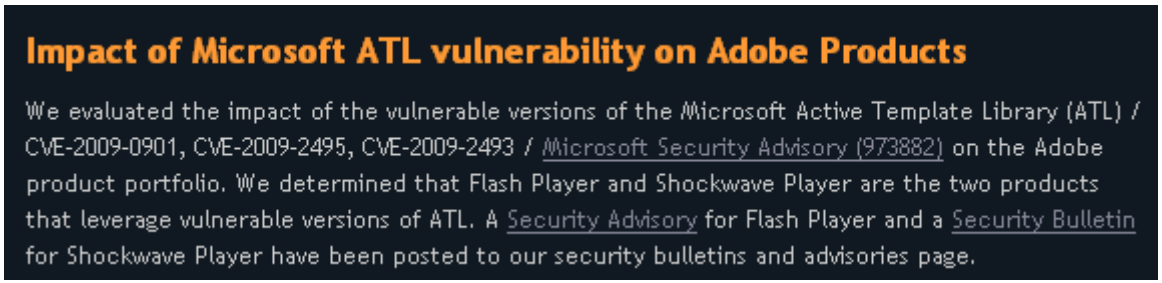
Delphi compilers were found to be infected with malware.

- »In fact even malware is found that is infected…

verizon business

Libraries and included foreign code

Most developers include standard available libraries and routines they did not built themselves. This can also result in turning your results from secure into insecure.



Impact of Microsoft ATL vulnerability on Adobe Products

We evaluated the impact of the vulnerable versions of the Microsoft Active Template Library (ATL) / CVE-2009-0901, CVE-2009-2495, CVE-2009-2493 / Microsoft Security Advisory (973882) on the Adobe product portfolio. We determined that Flash Player and Shockwave Player are the two products that leverage vulnerable versions of ATL. A Security Advisory for Flash Player and a Security Bulletin for Shockwave Player have been posted to our security bulletins and advisories page.

Microsoft Active Template Library issues

- Issues were found in header files of MS ATL.
- Everything built using these templates could now be vulnerable under specific conditions.
- Security and Hacker tools will and already do contain tests to find these weaknesses.

Again a reason to regularly check your developments, even if they are finished and in production.

Defaults of engines or middleware?

This happens all the time!

Make sure you test the things you depend on, and not just if it works as designed!

Look for defaults and security issues in the third-party components you use.

Hacker will see if it can be identified and will then look for known vulnerabilities..

Oh Nice! They are using a Firebird database engine. Does the default administrator password still work? YES!!

Overload? Step by Step? Timing?

It is nice if your application can handle the load that the functional specifications require, and maybe even some more….

– But have you checked just what happens if you push it too far?

3.7 Race Conditions

A race condition is anomalous behavior caused by the unexpected dependence on the relative timing of events. In other words, a programmer incorrectly assumed that a particular event would always happen before another.

Some of the common causes of race conditions are signals, access checks, and file opens. Signals are asynchronous events by nature so special care must be taken in dealing with them. Checking access with `access(2)` then `open(2)` is clearly non-atomic. Users can move files in between the two calls. Instead,

Timing issue example:

Incorrect implementation of two factor authentication

– Think of how to abuse…

– by first providing password and then code of an other token…

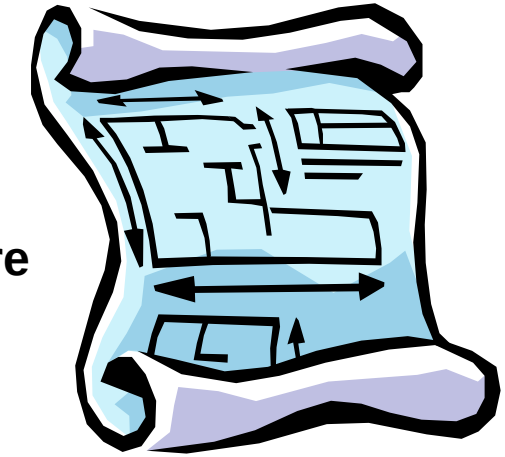
By the way: never assume authentication is finished…

verizon business

Wondering HOW or WHY opposed to IF…

Testing if something is validated is normal.

Figuring out HOW it is validated is something else…



- **Client Side validation works but is generally NOT secure**
  - Think about what parameters are used and can be abused.
  - Figure out how code at client side works and can be bypassed.
- **Foolproof mechanisms for preventing password reuse**
  - Nice, when I enter new password same as previous that is not allowed…
  - Now what if I keep on doing this?
- **Part of security testing mindset is:**
  - Reverse engineering.
  - Understanding how the programmer / designer works.
  - Thinking about how someone would support the application…

Would you consider what else your application could be used for?

What if your application can be used to access something outside your design?

– Who's problem is this?
– Testing for fail safe / fail closed.
– Means considering the future environment that is not part of the design or specifications.

Examples:

– Generation of an account statement in PDF for the customer. Nice that it could also be used to generate a PDF of every internal web server's default page.

– Email forms are frequently easy to abuse: sending mail elsewhere or pose as the application owner to the customer.

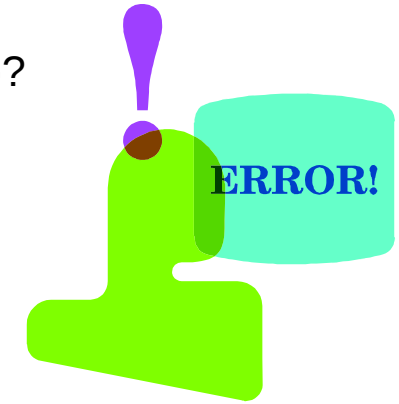
verizonbusiness

Do you check what error information is sent to user?

Naturally you want to be able to support customer if things do go wrong. Nice if customer gets a detailed message that can be sent to you…

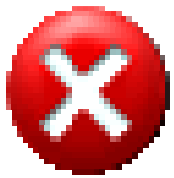
Security tester will need to consider:

- What information is presented here (system type, database layout)?
- What can it be used for? E.g. determine version of software?



Examples:

- SQL Injection and database enumeration.
- Sorry, username is ok but password is wrong…



Mindset: What about other mechanisms for the same issue?

How do you let someone recover a lost password?

verizon business

Other things to consider (1)

If there is time left (that would be a first…)

- **Do not blindly trust tools or applications. Make sure you know WHY something works correctly and keep updated to future issues!**
- **Toolbox and training of security tester is significantly different from application developer or functional tester.**
- **Where is the line between system tests, functional tests and integration in the production environment. Do you set requirements for these things?**
- **Covert channel & information combination can provide more information than intended by developer or the specifications.**

Other things to consider (2)

- Building blocks like Oracle introduce their own security requirements!
- Escaping a sandbox.
- Internet Explorer zones.
- Platform your application is installed on is not secured correctly…
- Walk away and think… Come back later!

Tips regarding mindset for security testing (1)

- Security testing in many cases is based on associative thinking. It cannot be completely scripted like functional testing.
- Because of creative or associative way of testing, methodology must be firmly managed to ensure areas are not skipped because of time restraints. Focus on high risk areas that were identified earlier.
- Security testing, especially if only done at the end of development, cannot be done by test-monkeys. And even worse, results are not always repeatable.
- Do research on all that is used to build the application. Stay up to date. And be curious! Read Read Read….
- There are many tools and many of them are very good… but tools do not replace someone with security testing experience.

Tips regarding mindset for security testing (2)

- The security tester should have the correct personality. Not everyone is equally suited for this task.
- Start testing as soon as possible during development and include security testers in early stages to spot development / design issues.
- Make sure the testers stay up to date. This means following daily security sites to identify if new methods of attack are discovered and relevant to your products.
- Know thy enemy! Follow a basic hacking course or read books on the subject. It will teach you to think outside your comfort zone (outside your specifications???)
- Train development staff and be prepared to manage pushback: “Hey, I was never asked to built something to prevent this? Why would someone want to do this?”

Where to go for more information

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

Information on the internet (just a selection)

- **Open Web Application Security Project (OWASP)**
  http://www.owasp.org/
  Their testing guide is a training in itself!
- **Secure Application Development**
  http://secappdev.org/
- **Safe Code**
  http://www.safecode.org/
- **Microsoft Security Development Lifecycle / Security Developer Center**
  http://msdn.microsoft.com/en-us/security/
- **The SANS institute**
  http://www.sans.org/

verizon business

Information from vendors and research companies

- **Research firms provide many excellent studies on differences in approach when adding security into software development processes:**
  - »Forrester
  - »Gartner
  - »Boston

- **Vendors of application security assessment tools provide excellent whitepapers** if you disregard the fact that their tool is the only real solution…

Code Review:
- »Fortify http://www.fortify.com/
- »Ounce Labs http://www.ouncelabs.com/

Vulnerability assessment for applications:
- »HP WebInspect
- »IBM AppScan

And the general vulnerability assessment tool vendors:
- »IBM ISS Internet Scanner
- »Qualys
- »Saint
- »Tenable Nessus

These are examples only, there is no intention to be complete and Verizon Business does not endorse any of these vendors or wants to expresses any preference!

Questions and Discussion

A Different Mindset for Testing

Functionality versus Security

August 27th 2009

verizonbusiness

Thank you for your attention!

Contact Details:

Email: rein.vankoten@verizonbusiness.com

Phone: +31 (0)6 55 787 495

R.J.C. (Rein) van Koten, CISA, CISSP, PCI-DSS QSA

Principal Consultant Information Security
Managing Consultant for PCI-DSS in Benelux & Middle East
Lead for Dutch Penetration Testing Team

Verizon Business Security Solutions powered by Cybertrust

verizonbusiness