



build | integrate | secure

Securing the SDLC: A Case Study

Texas Regional Infrastructure Security Conference (TRISC) 2008

Dan Cornell
April 22, 2008

Agenda

- Denim Group introduction and background
- The problem: Integrate security into the Denim Group SDLC
- How not to do it
- The solution: Fit to our organization
- Existing models for secure SDLC
 - *Microsoft SDL*
 - *Gary McGraw Security Touchpoints*
- Our starting point
- Steps taken so far
- Next steps
- Questions

Denim Group Overview

- Boutique IT consultancy
- Two sides of business:
 - *Software Development*
 - .NET
 - JEE
 - *Software Security*
 - Assessments and Penetration Tests
 - Code Reviews
 - Training
 - SDLC Consulting
- Consultants rotate between project types

Problem: Integrate Security into SDLC

- Business Reasons Why
 - *Organizations need reliable, secure systems*
 - *Software level attacks are a primary focus area for attackers*
 - *Presumably if you are at this talk to do not need to be sold on this...*
- (Semi-)Cynical Reasons Why
 - *Eat our own dog food*
 - *Practice what we preach*
- Ultimately: Make us better at what we do (software development and software security)

How Not To Do It

- Q: What are you all doing to address application security concerns in your organization?
- A: We bought “XYZ Scanner”
- Q: Okay... Are you actually using it?
- A: We ran some scans
- Q: And how did *that* go?
- A: Oh we found some stuff...
- Q: How did you address those issues?
- A: I think we sent the report to the developers. Not sure what they did with them. I guess I ought to check in on that...

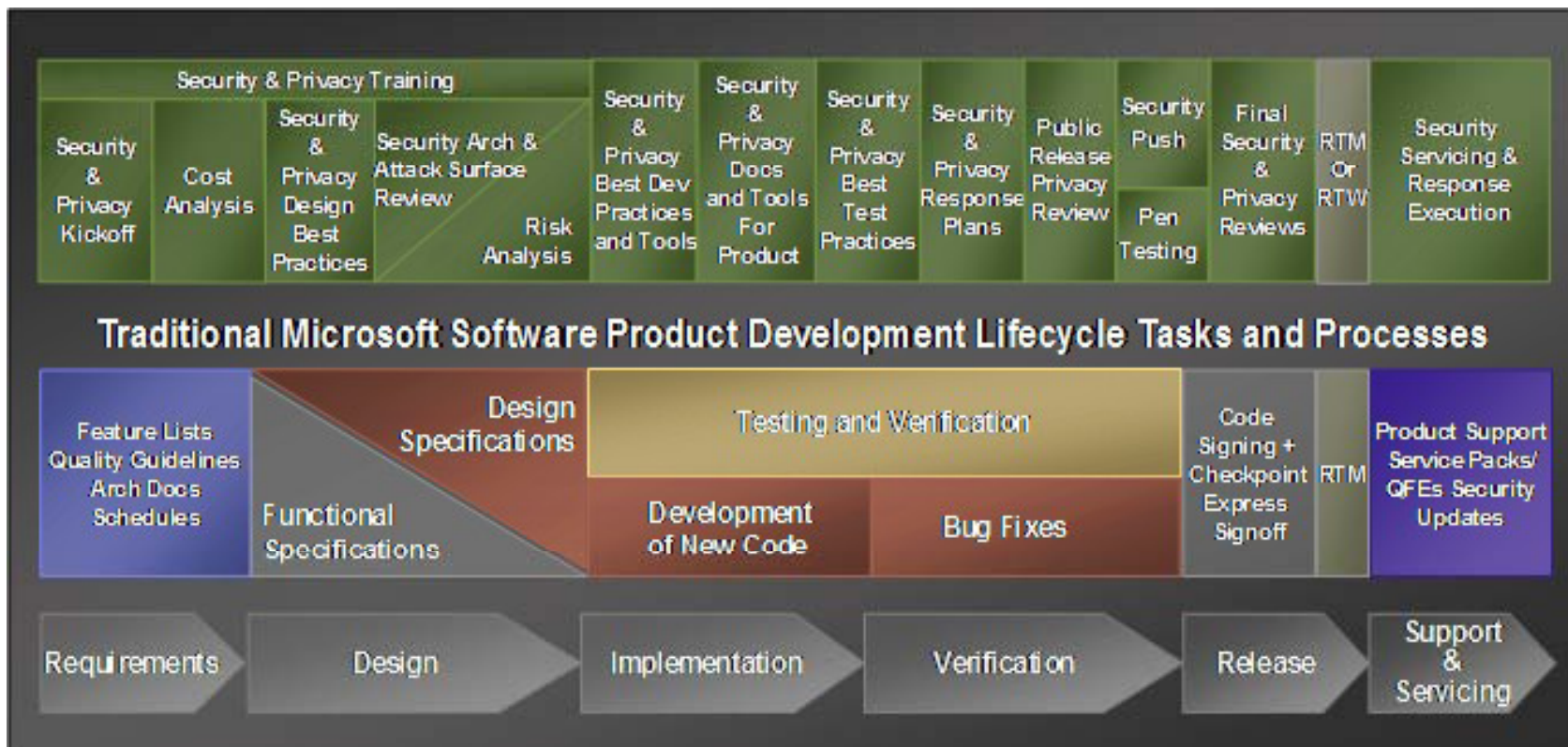
Solution

- Every organization is different
 - *Development practices: Agile, waterfall, cowboy-code*
 - *Control environment: Security, IT audit, compliance*
 - *Most important: Organizational values. What is important and how do things get done?*
 - *Not necessarily “Core Values” but certainly related*
- Denim Group:
 - *Intellectual curiosity*
 - “Students” of software engineering and construction
 - Multi-platform, multi-disciplinary
 - *Billability*
 - If our people are billing then making payroll is easy
 - *Do not compete on price, but be market-responsible*
- You must overcome resistance (even at Denim Group)

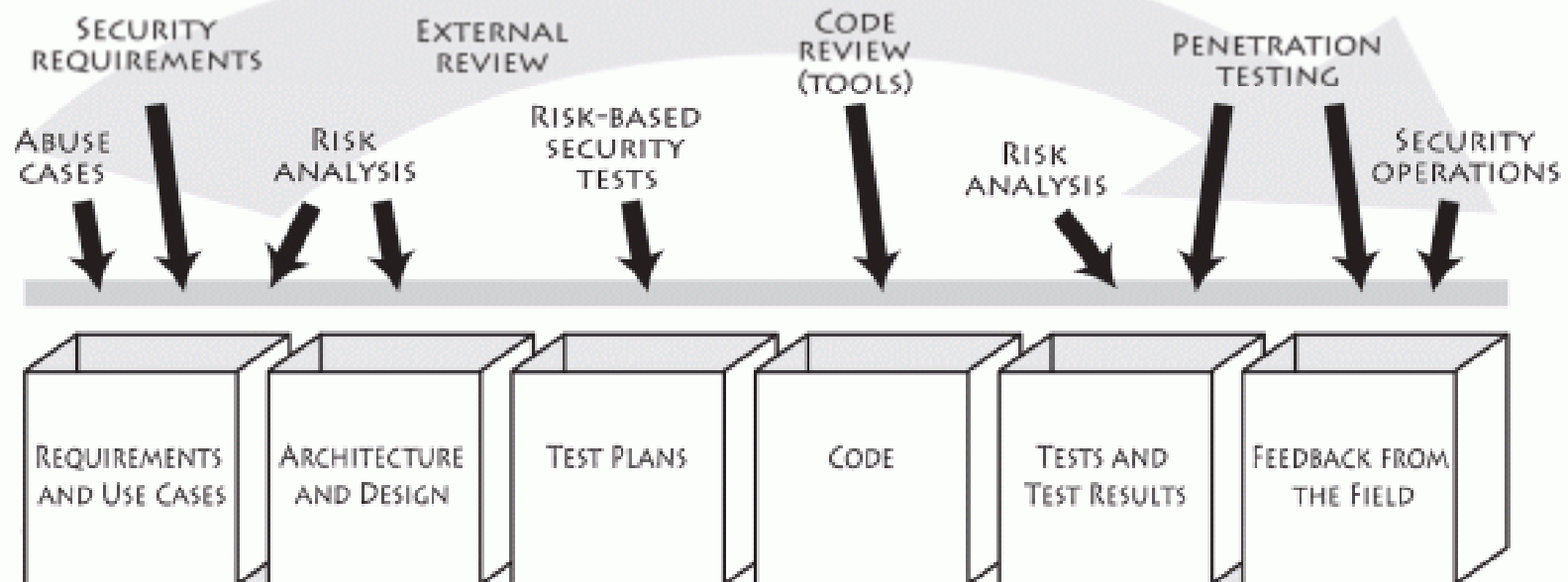
Existing Models

- Microsoft SDL
- Gary McGraw Security Touchpoints

Microsoft SDL



Gary McGraw Security Touchpoints



Framework

- People
- Processes
- Technologies

Starting Point

- Culture of learning
 - *Versatility is a great asset in our organization – lots of cross training*
 - *Lunch and learn program*
 - *Certification study groups*
- Requirements development
 - *Project Vision Document*
 - *Functional Specification Document*
 - *Or two week iterations for Agile projects*
- Lots of automated testing
 - *Unit testing*
 - *Acceptance testing*
- Continuous integration

Steps Taken So Far

- Secure application development training (people)
- Up front risk analysis (process)
 - *Abuse cases, architectural risk analysis, security requirements*
- Static analysis (technology)
- Real time analysis distributed with binaries (technology)

Secure Application Development Training

- We provide this training for our clients
 - *Great opportunity for us to develop our people and improve our training content at the same time*
- Classes run in-house during lunches
 - *Fundamental of application security*
 - *OWASP Top 10*
 - *Application assessment and penetration testing*
 - *Security source code reviews*
- Run through the series of training modules then start over
 - *Address new team members and individuals who missed modules due to being absent while on engagements*
- Looking to incorporate e-learning as well

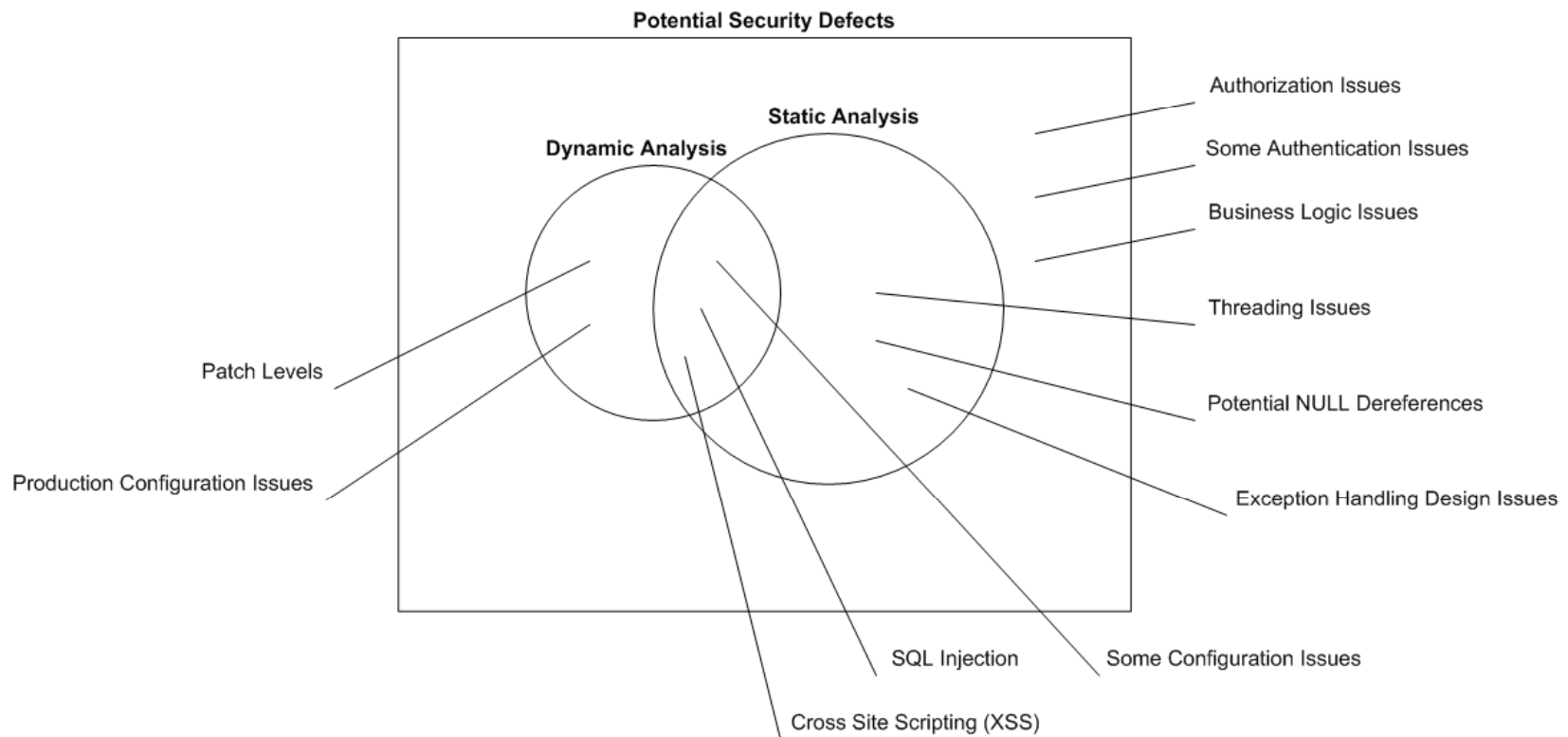
Up Front Risk Analysis

- Components
 - *Abuse cases*
 - *Architectural Risk Analysis (Threat Modeling)*
 - *Security Requirements*
- Done informally on a per-project basis
 - *Only works because of security aware culture*
- Online game: detect and stop cheaters
- Medical records application: encryption standards
- Online loan application: encryption standards
- Social network application: Handling potentially malicious content

Static Analysis

- Started with FindBugs, PMD, FxCop
- Recently deployed Fortify SCA

Dynamic, Static and Manual Testing



Denim Group Decision

- Most of our folks are software developers
- We have full access to all the code (we write it...)
- We are primarily responsible for the code and less responsible for the deployed environment
- Therefore: Static Analysis
- Looking to add Dynamic Analysis in the future

Deploying a Tool

- Questions
 - *Who will run the tool?*
 - *When will it be run?*
 - *What will be done with the results?*
- If you haven't answered these – don't waste your money on a tool
 - *It won't be used*
 - *Nothing will be done with the results*
 - *However you may fool your auditors...*

Static Analysis at Denim Group: WHO

- At Denim Group, consultants rotate between development and QA roles
- All consultants are trained to use the tools
 - *External security source code review*
 - *Scan the code they write*
 - *Scan the code they are providing QA for*
- QA team for the project are the actual gatekeepers

Static Analysis at Denim Group: WHEN

- Run informally via the IDE by developers to identify issues before someone else finds them
- Integrated into nightly build

Static Analysis at Denim Group:

WHAT

- Don't argue about exploitability – just fix the @\$%! Issue
 - *Scheduled bug fixing “sprints” (1-4 hours) – great for squashing bugs, tough for end to end metric tracking*
- HOT defects must be fixed or signed off on by a Principal OR by the Director of Technology
- WARNING defects must be fixed or signed off on by the Project Lead AND the QA Lead
- We have an advantage over many organizations because our application portfolio rolls over periodically

Real Time Analysis with Binaries

- RTA technology distributed with all JEE and .NET binaries
- Protects against some variants of many common attacks
 - *SQL injection*
 - *Cross Site Scripting (XSS)*
- More important – provides information about attacks in progress
- Trial license

Next Steps

- Additional documentation
- Application portfolio management
- Dynamic analysis tools
- Formal application assessments

Additional Documentation

- Consistently augment our PVDs and FSDs with specific security requirements
- Must be done in project budget-responsible manner

Application Portfolio Management

- Start to track some metrics and trending

Dynamic Analysis Tools

- We use them for our assessments and penetration tests
- Would provide additional coverage for our security testing

Formal Assessments

- Have QA perform actual application assessments according to our externally-facing methodology
 - *Done informally right now*
- Scheduled WBS item
- Must address Critical and High issues before release

Conclusions

- Good progress made
 - *Security aware culture*
 - *Security trained developers*
 - *Security requirements addressed up front*
 - *Static analysis helps baseline code security*
- Still more to do
 - *Formalize documentation*
 - *Consistency*

Questions?

Dan Cornell

dan@denimgroup.com

Web: www.denimgroup.com

Blog: denimgroup.typepad.com