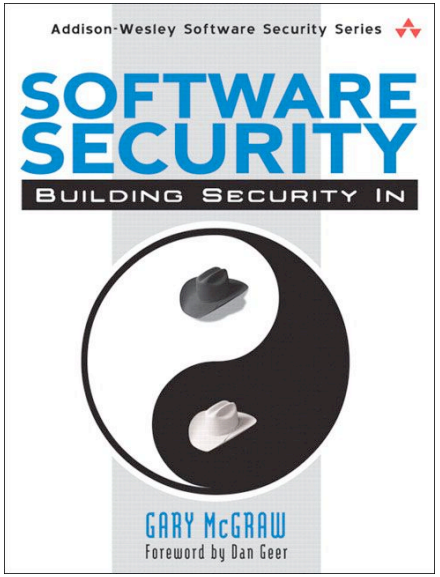
Software Security: State of the Practice 2009

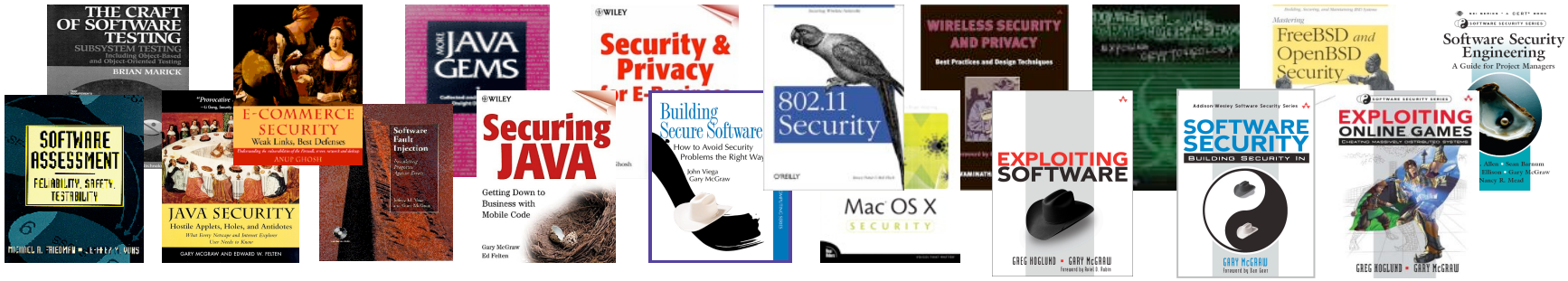
Gary McGraw, Ph.D.
Chief Technology Officer, Cigital

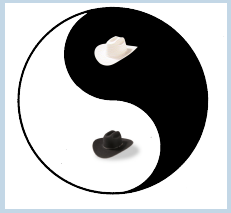


cigital

Cigital

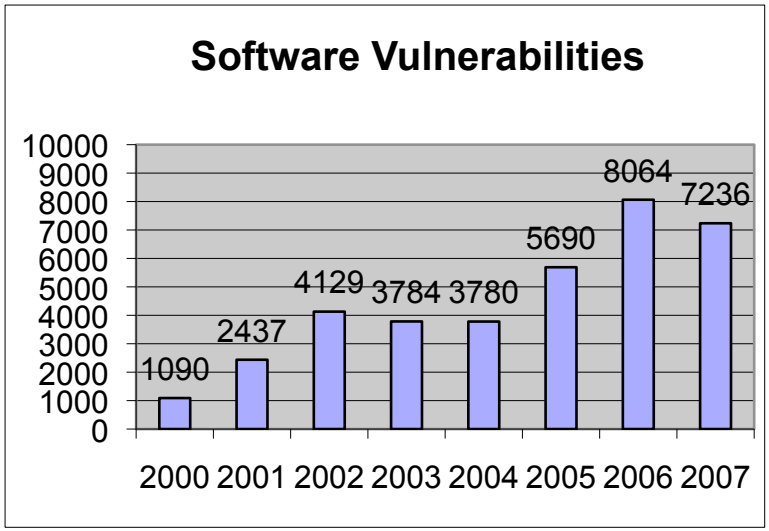
- Founded in 1992 to provide software security and software quality professional services
- Recognized experts in software security and software quality
  - Widely published in books, white papers, and articles
  - Industry thought leaders

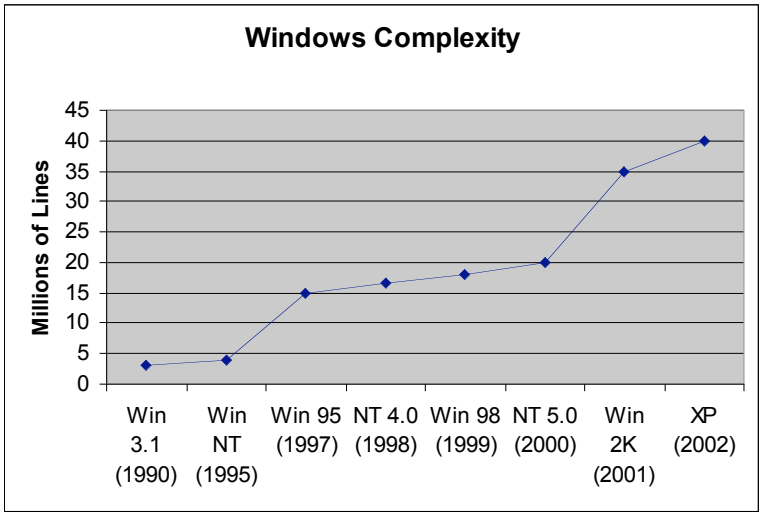


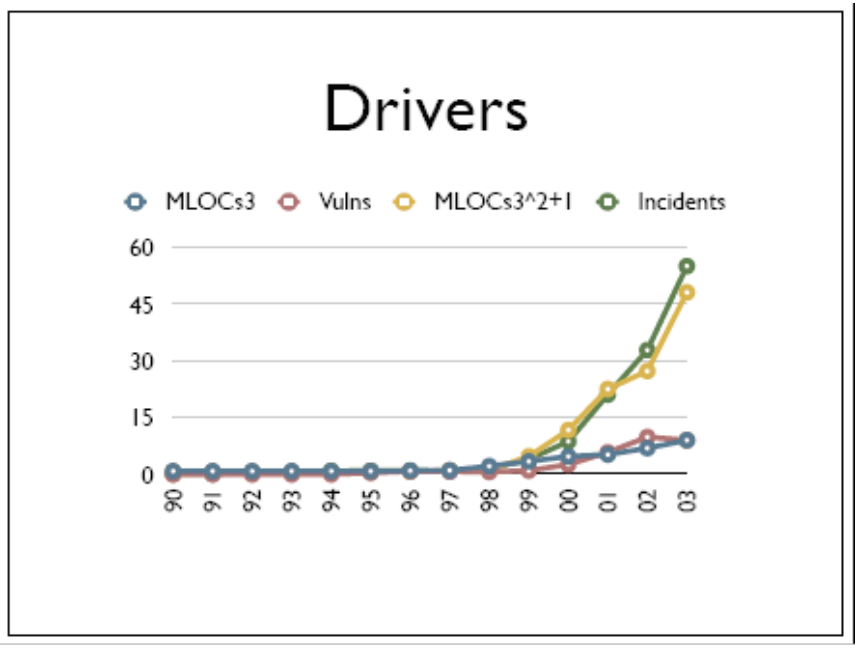


Awareness

Monoculture sinks in







cigital

Security as a differentiator

- Apple sells iMac and MacBook with security
- Firefox sells browser with security

Diversity works

- We see both .NET and J2EE
- We see Oracle, SQL, and DB2
- We see Unix, Linux, AIX, Windows, OSX
- All in the same location

Firefox
rediscover the web

cigital

The rise of the software security group

- Cigital SSG turns ten
- Microsoft adopts the Secure Development Lifecycle
- Many companies have a group devoted to software security

- microsoft
- dtcc
- emc
- fidelity
- adobe
- wells fargo
- goldman sachs
- google
- qualcomm
- morgan stanley
- USAF
- dell
- cisco
- bank of america
- walmart
- finra
- vanguard
- college board
- oracle
- state street
- omgeo
- motorola
- general electric
- lockheed martin

cigital

Conferences and magazines for swsec

- SD Best Practices keynote is software security
- SD West security track matures
- OWASP conferences (for practitioners)
- Star West and FutureTest teach security to testers

- IEEE Building Security In enters 5th year

SD BEST PRACTICES 2006 CONFERENCE & EXPO

STAR WEST

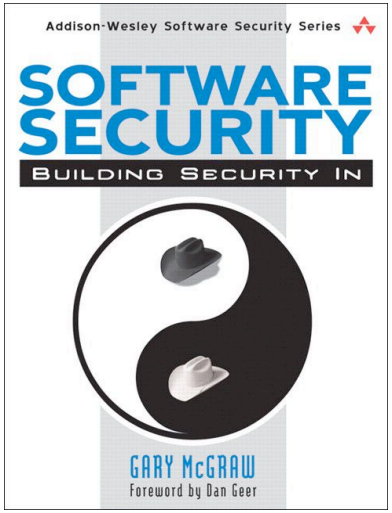
SD WEST 2006 Software Development Conference & Expo
March 13-17, 2006
Santa Clara Convention Center
Santa Clara, CA

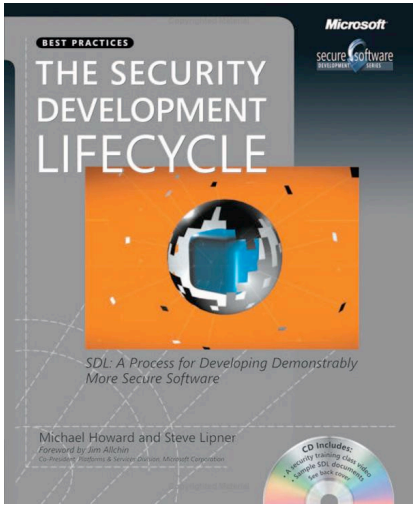
IEEE SECURITY & PRIVACY

cigital

A shift from philosophy to HOW TO

- Integrating best practices into large organizations
  - Microsoft's SDL
  - Cigital's touchpoints
  - OWASP adopts CLASP





What works: BSIMM

- Building Security In Maturity Model
- Real data from real initiatives

The software security market grows (2006-7)

Software security [$55M→91.9M]

- Fortify [$15.9M→29.2M]
- Secure Software (Fortify) [$2M]
- Ounce Labs [$3.1M→9.5M]
- Coverity [$18M→27.2M]
- Klokwork[$16M→26.0M]

Application security [$80-100M→150-180M]

- IBM/Watchfire [$26M→24.1M]
- HP/SPI Dynamics [$21.2M→22.3M]
- Cenzic, Codenomicon, Whitehat, … [$12.5M]

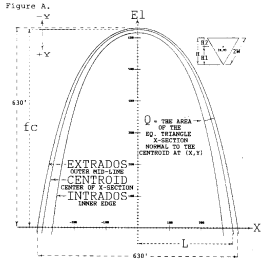
Application firewalls [$30M→50M]

- Software security services both around tools and other assessments [$100M→100-140M]
  - Cigital, Foundstone, E&Y, IBM, Cybertrust

- Yankee group 2006 estimate $250-275M
- 2007 estimate = $390-460M
- http://www.informit.com/articles/article.aspx?p=1237978

badness-ometers lead to awareness

The bugs/flaws continuum



`gets()`

`attacker in the middle`

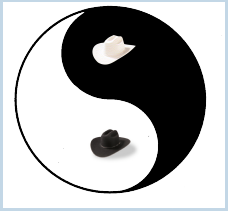
BUGS — FLAWS

- Architectural risk analysis
- Customized static rules (Fidelity)
- Commercial SCA tools: Fortify, Ounce Labs, Coverity
- Open source tools: ITS4, RATS, grep()

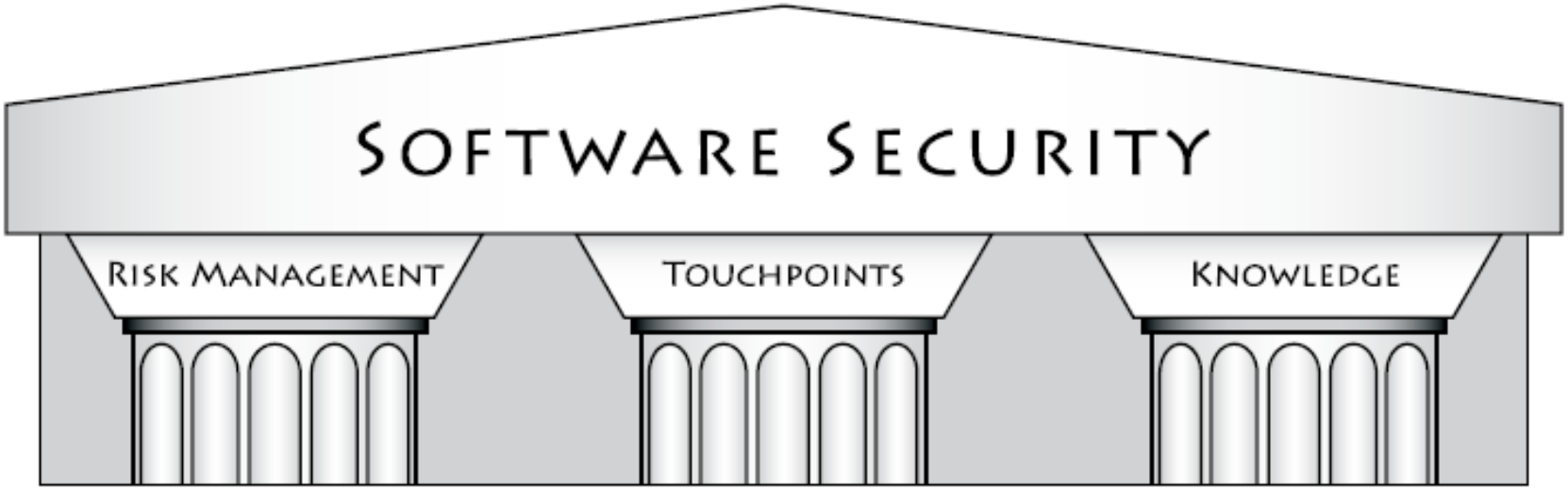
cigital

Software security common sense

- Software security is more than a set of security functions
  - Not magic crypto fairy dust
  - Not silver-bullet security mechanisms
- Non-functional aspects of design are essential
- Bugs and flaws are 50/50
- Security is an emergent property of the entire system (just like quality)
- To end up with secure software, deep integration with the SDLC is necessary

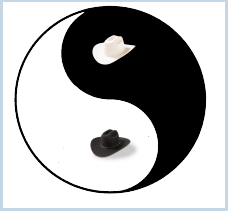


Three Pillars of Software Security



Three pillars of software security

- Risk management framework
- Touchpoints
- Knowledge



Risk Management Framework

cigital

Why risk management?

- Business understands the idea of risk, even software risk
- Technical perfection is impossible
  - There is no such thing as 100% security
  - Perfect quality is a myth
- Technical problems do not always spur action
  - Answer the “Who cares?” question explicitly
- Help customers understand what they should *do* about software risk
- Build better software

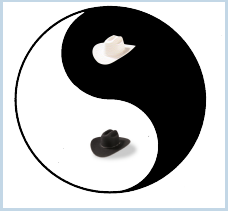
Who cares?

cigital

Financial vertical leads the pack

- All major investment banks have a Chief Risk Officer
  - SOX caused banks to realize their software risk
  - Software security initiatives resulted
- Credit card consortiums recognize software security in PCI standards
- Software vendors and high tech companies have a much harder time connecting to business

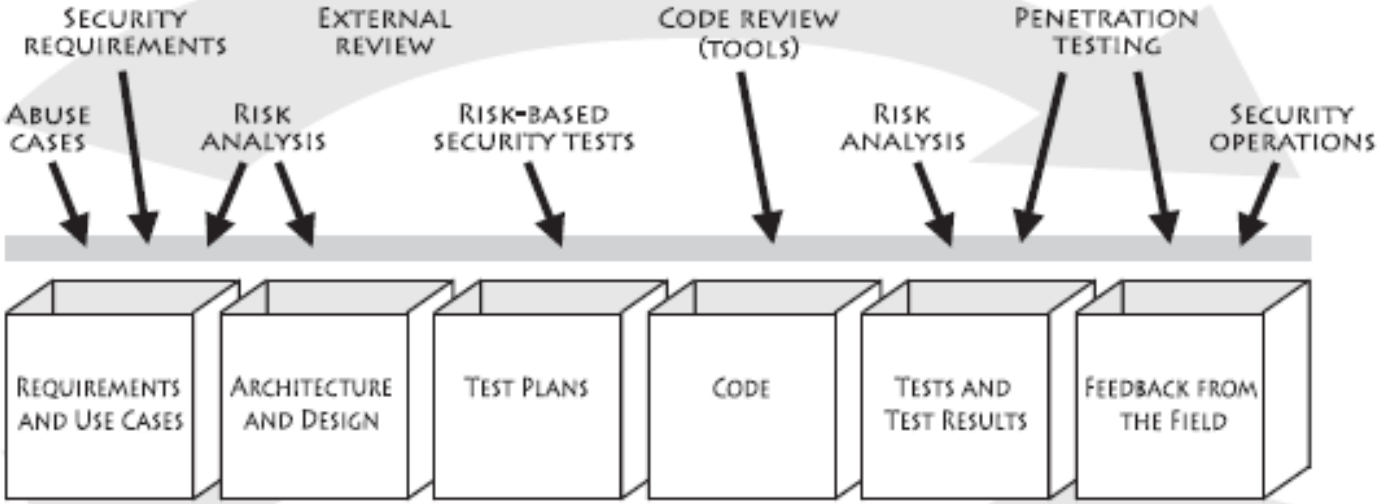
PCI Security Standards Council™



Software Security Touchpoints

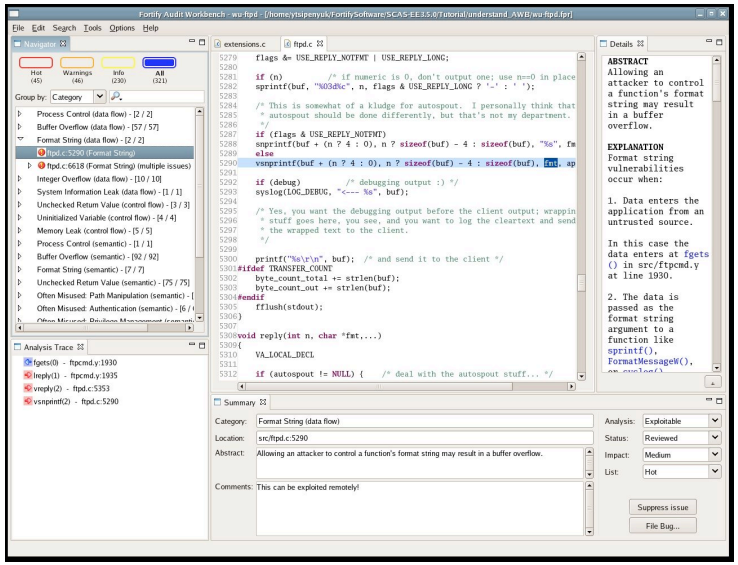
cigital

Software security touchpoints



cigital

Touchpoint: Code review (with a tool)



- Code scanning catches on
  - Demand for manual services up
  - Tool adoption proceeding apace (being measured)
- Tools (finally) handle large code bases
  - Don't fail to grep()
  - Simple enforcement is no longer useful
- Customization pays off royally
  - Fidelity
  - DTCC

- Training courses about bugs and tools widespread

FORTIFY

coverity

OUNCE LABS

cigital

Fidelity leads the pack

- Corporate-wide adoption of the tool
- Creation of rules
  - Corporate standards enforcement (DES vs 3DES)
  - Custom rules push past the tool's natural limits
  - Custom rules look at more constraints surrounding a particular code construct (false positives drop)
- Application assessment factory
  - Code that builds in
  - Actionable bugs out
  - Hide the assembly line behind an API for better management

  - http://www.informit.com/articles/article.aspx?p=1231818

Fidelity INVESTMENTS

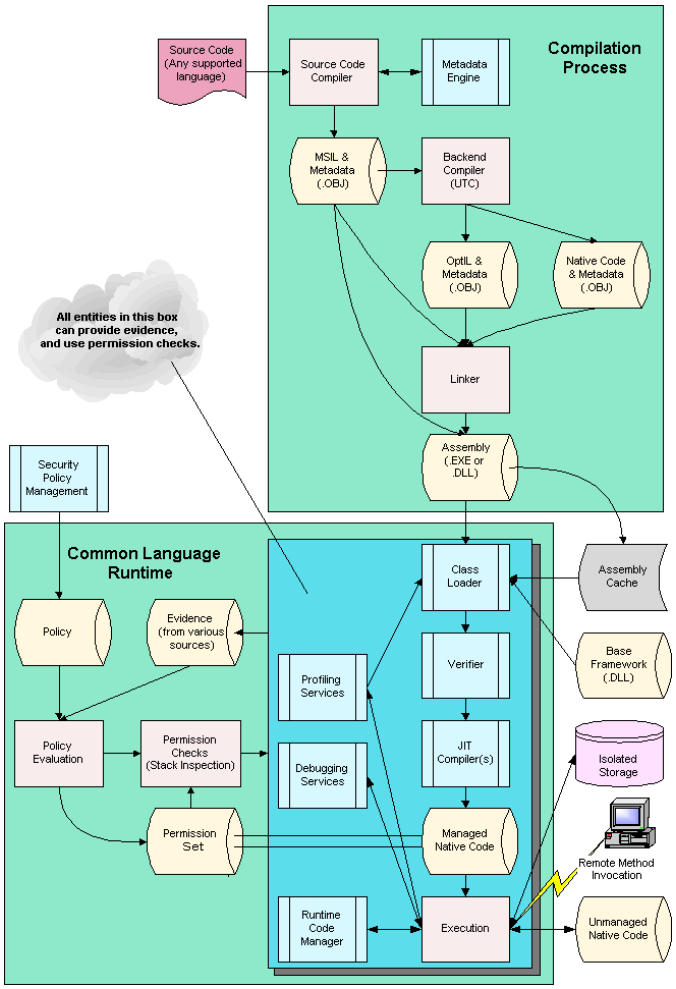
Example: constructing a factory

- Automating the line itself not just factory workers
  - Use Cruise Control as assembly line
  - Use Subversion to store and diff submissions
- Replace factory workers with under-utilized robots
  - Tune Fortify
  - Make great use of pen test tools
- Integrate new robots
  - Ounce5
  - Breach Web Defend
  - Script checks if necessary

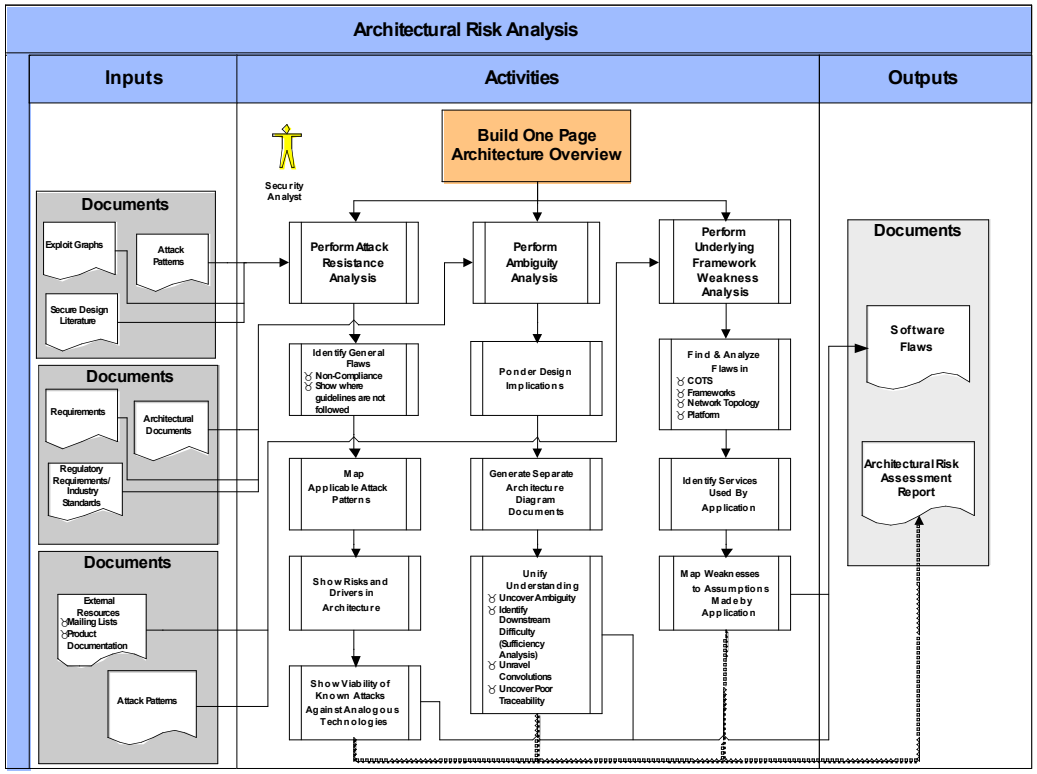
Touchpoint: Architectural risk analysis

- More common to find customers with a handle on software architecture
- Widespread use of common components
  - Spring
  - Hibernate
  - Log4J
  - OpenSSL
  - “ripple effect”
- Design patterns help

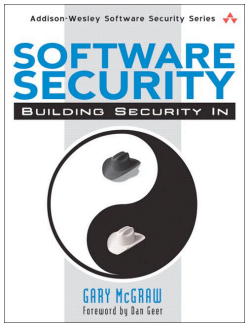
- High-expertise work is still hard to teach
- Training courses about ARA just being adopted



Touchpoint: Architectural risk analysis



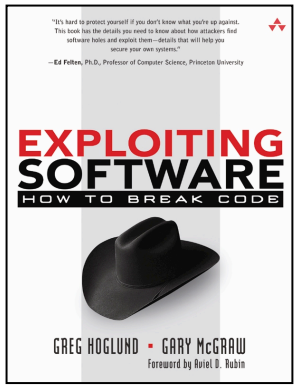
- Start by building a one-page overview of your system
- Then apply the three-step process we will describe more fully later
  - Attack resistance
  - Ambiguity analysis
  - Weakness analysis



cigital

Touchpoint: Penetration testing

- Penetration testing finds its place
  - Badnessometer (helpful for booting program)
  - Solutions more important than finding problems
- Focus on final software environment
  - Configuration
  - Context
- Clients no longer rely on pen tests exclusively



cigital

Touchpoint: Security testing

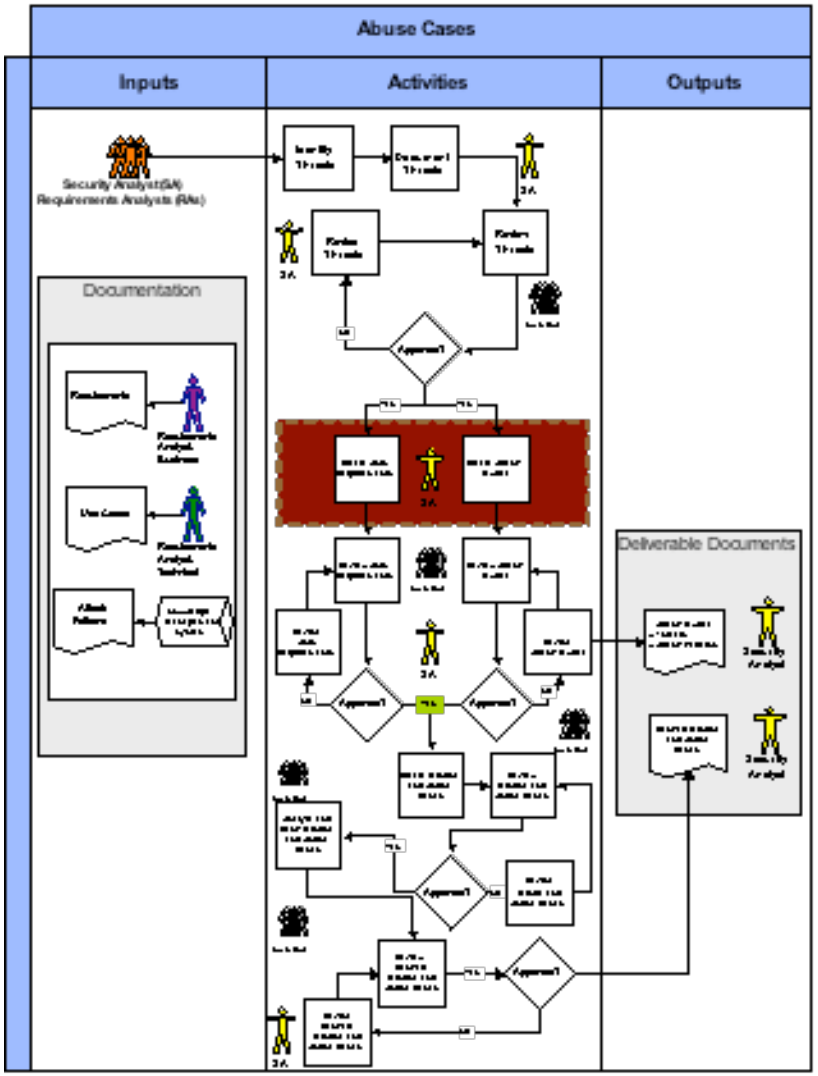
- Test security functionality
  - Cover non-functional requirements
  - Security software probing
- Risk-based testing
  - Use architectural risk analysis results to drive scenario-based testing
  - Concentrate on what “you can’t do”
  - Think like an attacker
  - Informed red teaming
- Training on security testing begins
- SQE offers public training courses
- Keynote at major testing conference is security

cigital

Touchpoint: Abuse cases

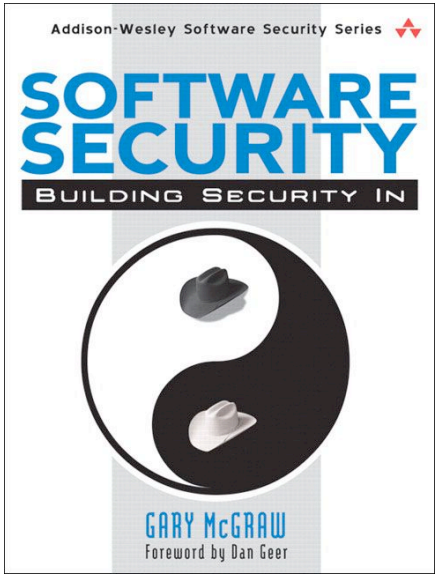
- Abuse cases used in DARPA work to drive requirements of advanced security system
- The problem of “implicit requirements” remains widespread
- Training: course development and delivery is nascent

DARPA ITO
Information Technology Office.

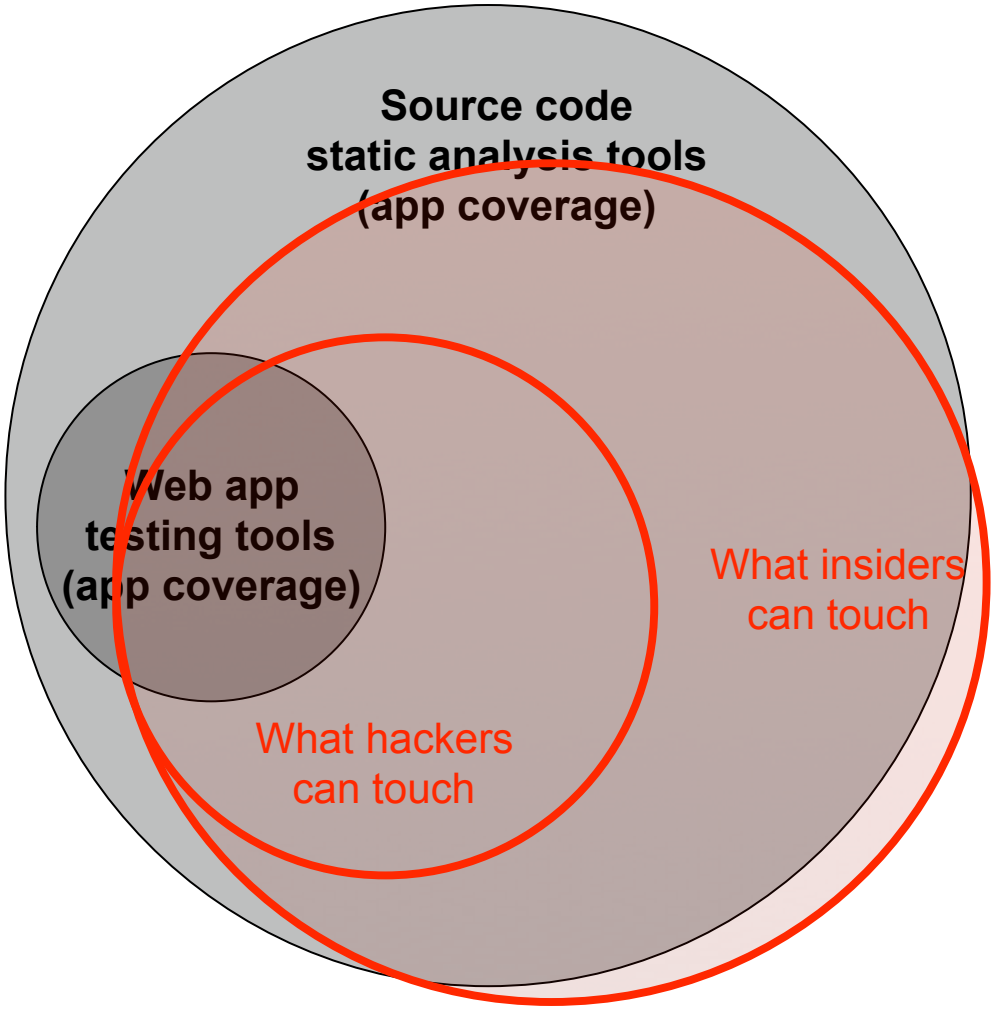


Touchpoint: Abuse cases

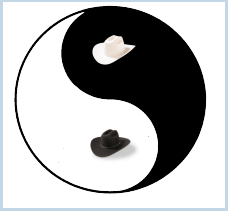
- Starting with attack patterns, requirements and use cases
- Identify anti-requirements
- Build an attack model
- Determine misuse and abuse cases



Software security tools: app coverage



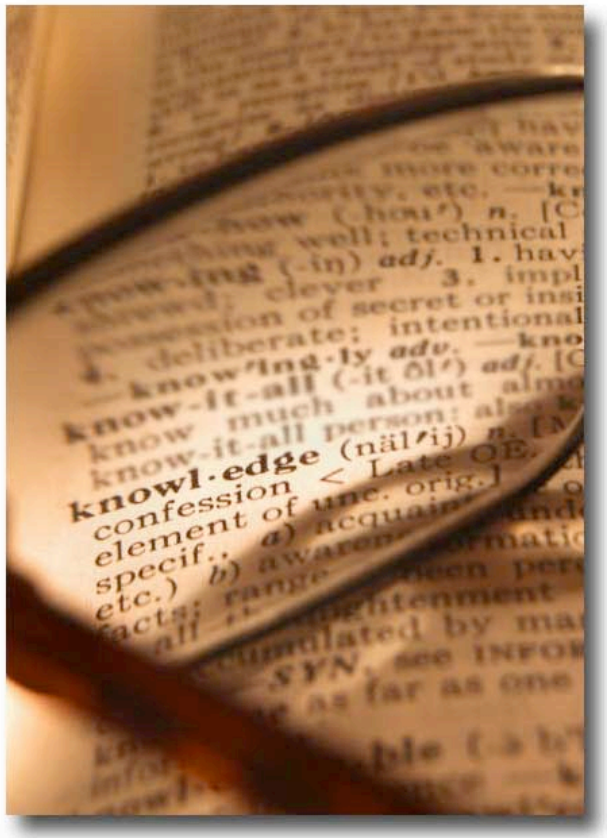
- Black box web testing tools only cover Web software
  - Useful for QA
- White box analysis tools cover a much larger set of software
  - Require clue about code



Knowledge

cigital

Knowledge catalogs



- Principles
- Guidelines
- Rules
- Attack patterns
- Vulnerabilities
- Historical Risks

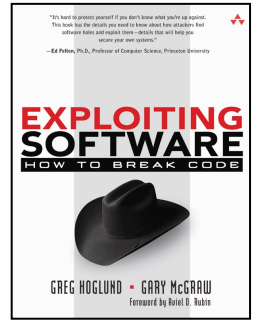
Enterprise knowledge bases

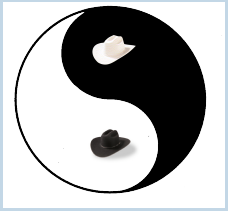
- Corporate standards get smart
  - Written in code
  - Enforceable by tools
- Knowledge makes the round trip
  - What we see in scans
  - What goes into training
  - How we build code standards
  - What the tools enforce
- Fidelity identifies Common Vulnerability Patterns

cigital

Attack patterns

- Make the Client Invisible
- Target Programs That Write to Privileged OS Resources
- Use a User-Supplied Configuration File to Run Commands That Elevate Privilege
- Make Use of Configuration File Search Paths
- Direct Access to Executable Files
- Embedding Scripts within Scripts
- Leverage Executable Code in Nonexecutable Files
- Argument Injection
- Command Delimiters
- Multiple Parsers and Double Escapes
- User-Supplied Variable Passed to File System Calls
- Postfix NULL Terminator
- Postfix, Null Terminate, and Backslash
- Relative Path Traversal
- Client-Controlled Environment Variables
- User-Supplied Global Variables (DEBUG=1, PHP Globals, and So Forth)
- Session ID, Resource ID, and Blind Trust
- Analog In-Band Switching Signals (aka “Blue Boxing”)
- Attack Pattern Fragment: Manipulating Terminal Devices
- Simple Script Injection
- Embedding Script in Nonscript Elements
- XSS in HTTP Headers
- HTTP Query Strings
- User-Controlled Filename
- Passing Local Filenames to Functions That Expect a URL
- Meta-characters in E-mail Header
- File System Function Injection, Content Based
- Client-side Injection, Buffer Overflow
- Cause Web Server Misclassification
- Alternate Encoding the Leading Ghost Characters
- Using Slashes in Alternate Encoding
- Using Escaped Slashes in Alternate Encoding
- Unicode Encoding
- UTF-8 Encoding
- URL Encoding
- Alternative IP Addresses
- Slashes and URL Encoding Combined
- Web Logs
- Overflow Binary Resource File
- Overflow Variables and Tags
- Overflow Symbolic Links
- MIME Conversion
- HTTP Cookies
- Filter Failure through Buffer Overflow
- Buffer Overflow with Environment Variables
- Buffer Overflow in an API Call
- Buffer Overflow in Local Command-Line Utilities
- Parameter Expansion
- String Format Overflow in syslog()





Enterprise Initiatives and the BSIMM

cigital

The process: choosing the nine

- Big idea: Build a maturity model from actual data gathered from 9 of 25 known large-scale software security initiatives

- Create software security framework
- Nine in person executive interviews
- Build bullet lists (one per practice)
- Bucketize the lists to identify activities
- Create levels
  - Objectives → Activities
  - 110 activities supported by real data
  - Three levels of “maturity”

cigital

Real world data: the nine

- Initiative age 5yrs 4months
  - Newest 2.5
  - Oldest 10
- SSG size 41
  - Smallest 12
  - Largest 100
  - Median 35
- Satellite size 79
  - Smallest 0
  - Largest 300
  - Median 20
- Dev size 7750
  - Smallest 450
  - Largest 30,000
  - Median 5000

cigital

A Software Security Framework

Governance	Intelligence	SDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

- Four domains
- Twelve practices
- See informIT article
- http://www.informit.com/articles/article.aspx?p=1271382

cigital

Ten surprising things

1. Bad metrics hurt
2. Secure-by default frameworks
3. Nobody uses WAFs
4. QA can't do software security
5. Evangelize over audit
6. ARA is hard
7. Practitioners don't talk attacks
8. Training is advanced
9. Pen testing is diminishing
10. Fuzz testing

- http://www.informit.com/articles/article.aspx?p=1315431

cigital

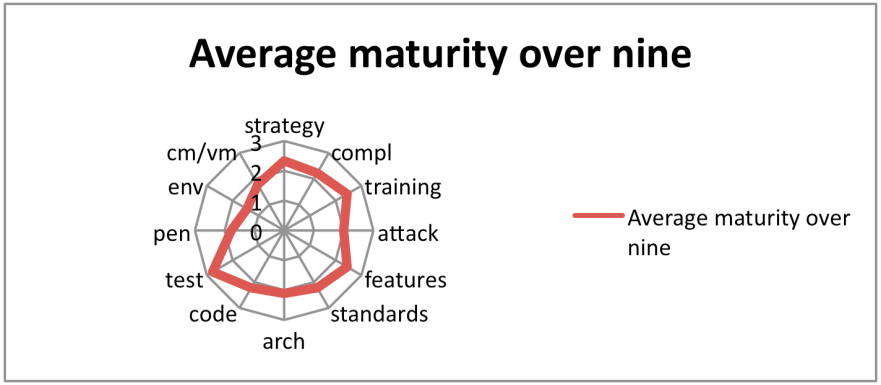
SSMM

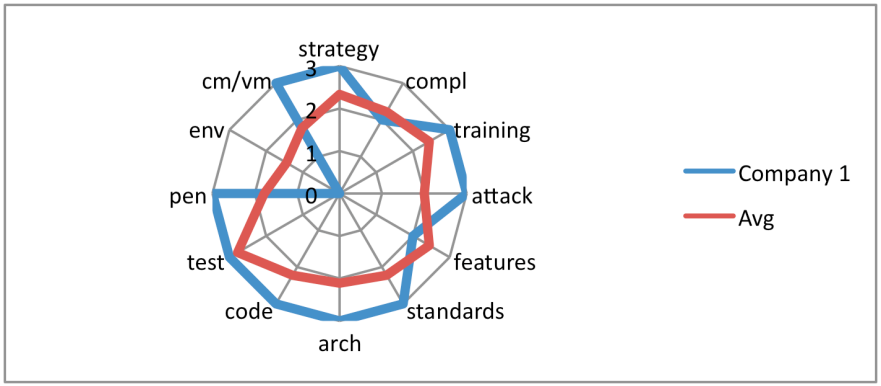
- SAMM beta is under review (release next week)
- Top-down presentation through GOALS and OBJECTIVES
- 110 activities with examples
- Three levels of maturity
- How to use the model

- Where do you stand?
- What should you do next?

The Nine (where you stand)

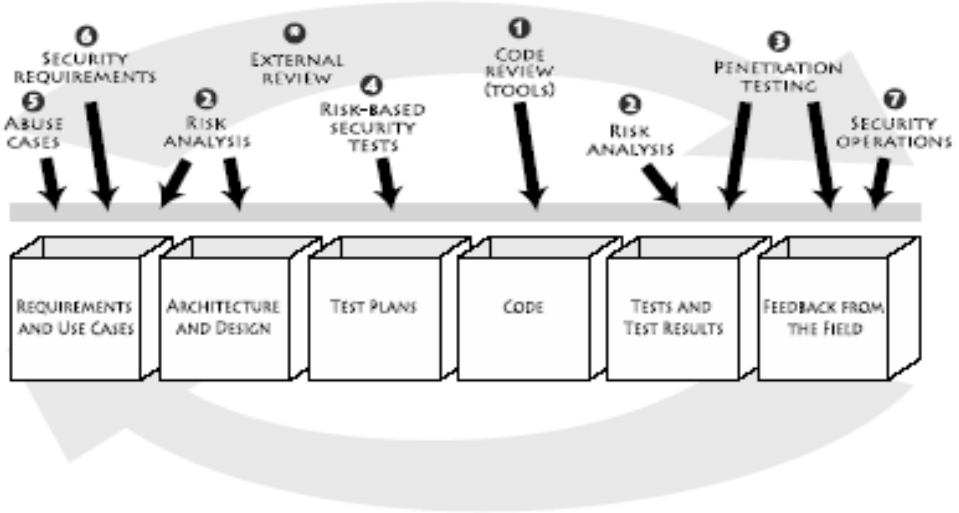
- Activities that ALL do
  - evangelist role
  - policy
  - awareness training
  - history in training
  - security features
  - SSG does ARA
  - black box tools
  - external pen testing
  - good network security





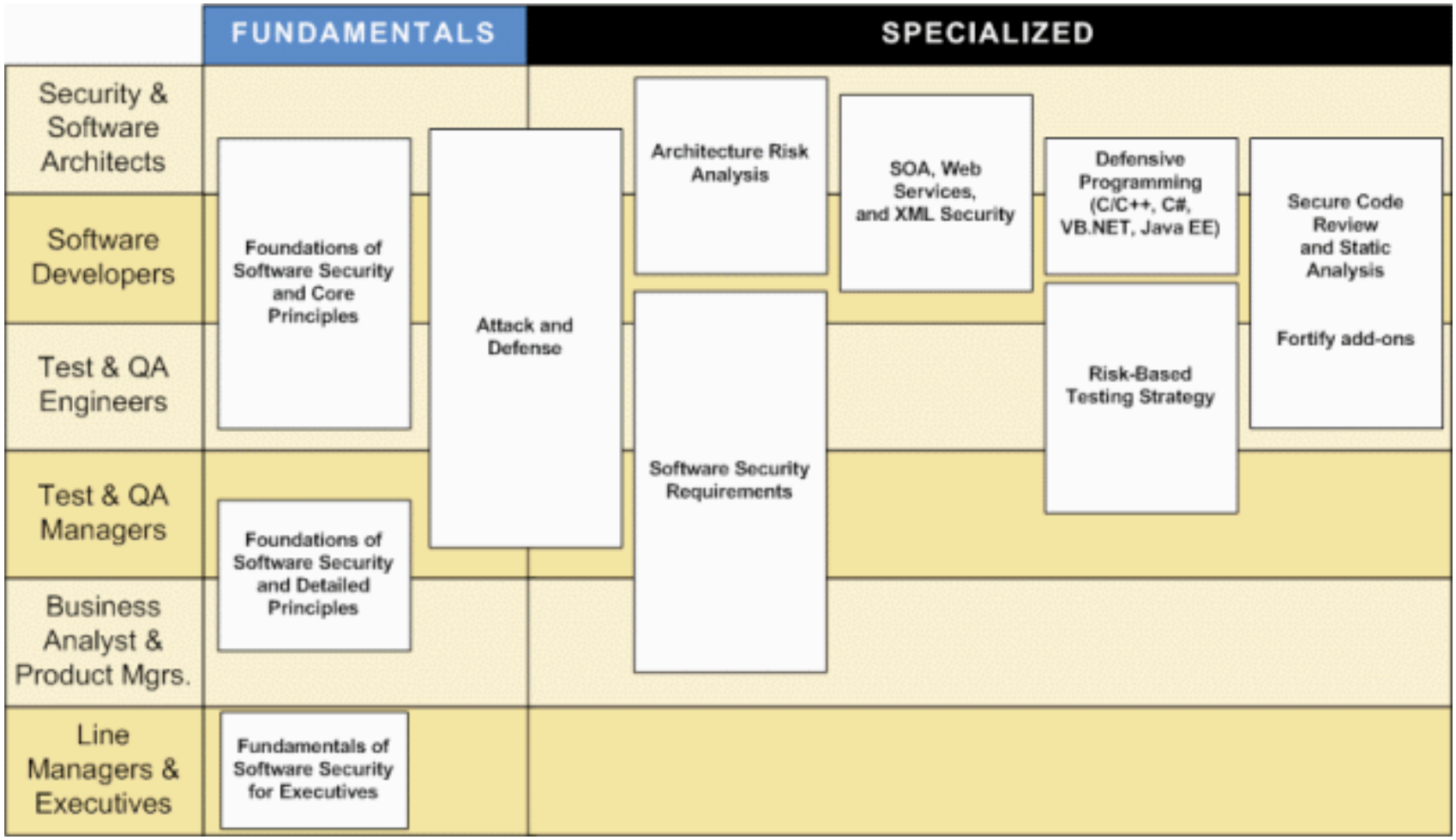
Touchpoints adoption

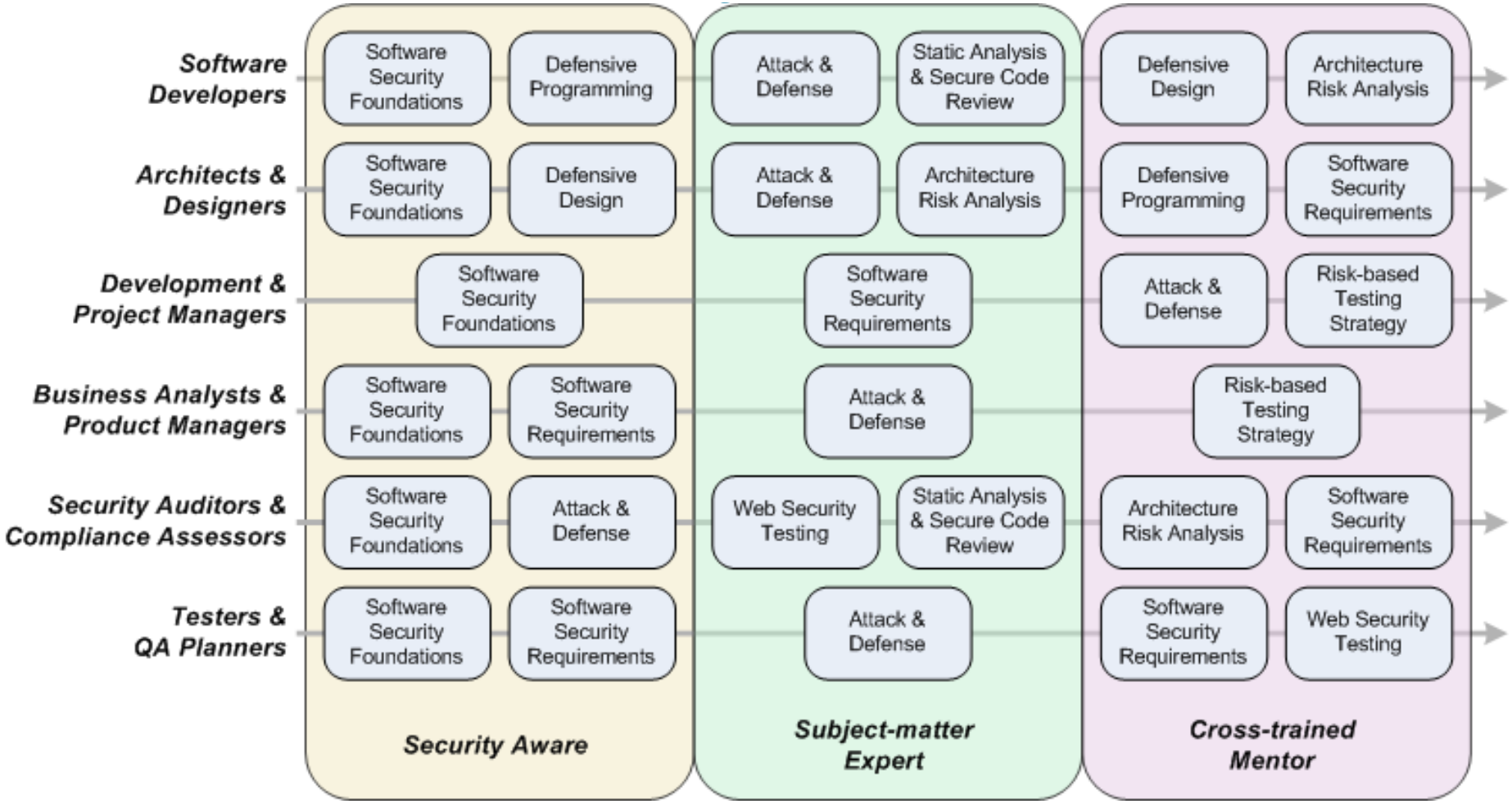
- Code review
  - Widespread
  - Customized tools
  - Training
- ARA
  - Components help
  - Apprenticeship
  - Training
- Pen testing
  - No longer solo
- Security testing
  - Training
- Abuse cases and security requirements
  - Training



cigital

Beyond awareness training



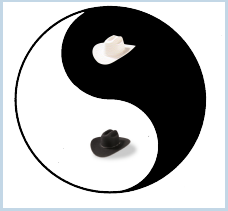


cigital

Four ways to start

- Top-down framework
  - Strong centralized IT leadership
- Portfolio risk
  - Stove-piped business units
- Training first
  - Technical world led by dev
- Lead with a tool
  - Technical world led by QA/app security

- See darkreading column “Software Security Strategies”
  http://www.darkreading.com/document.asp?doc_id=142829



Where to Learn More

cigital

informIT & Justice League

informIT

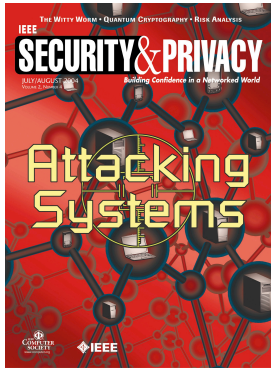
- www.informIT.com
- No-nonsense monthly security column by Gary McGraw

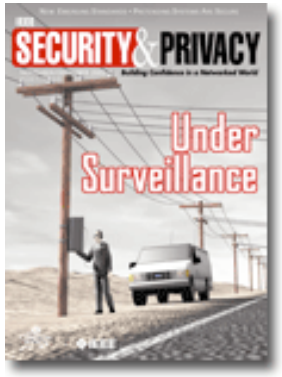
- www.cigital.com/justiceleague
- In-depth thought leadership blog from the Cigital Principals
  - Scott Matsumoto
  - Gary McGraw
  - Sammy Migues
  - Craig Miller
  - John Steven

IEEE Security & Privacy Magazine + 2 Podcasts

- Building Security In
- Software Security Best Practices column edited by John Steven
- www.computer.org/security/bsisub/

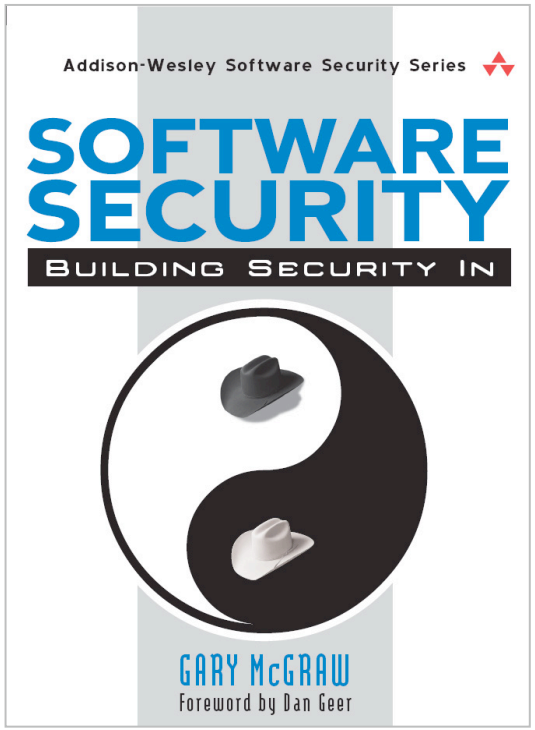
The Silver Bullet Security Podcast with Gary McGraw





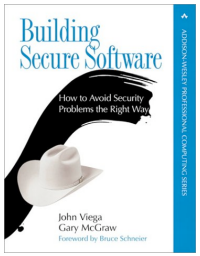
- www.cigital.com/silverbullet
- www.cigital.com/realitycheck

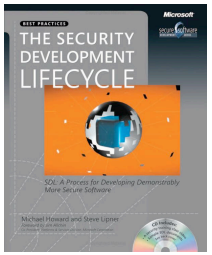
cigital

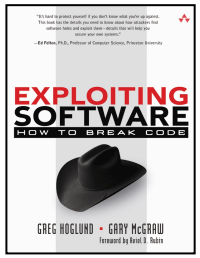


Software Security: the book

- How to DO software security
  - Best practices
  - Tools
  - Knowledge
- Cornerstone of the Addison-Wesley Software Security Series
- www.swsec.com



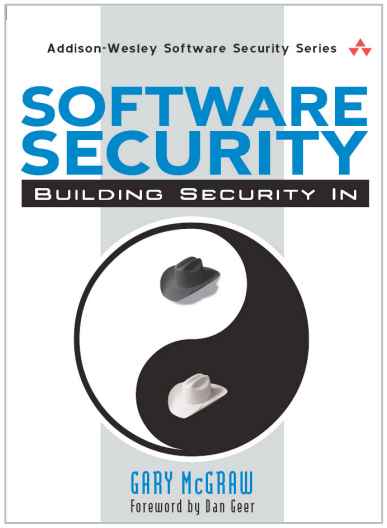




Addison Wesley

cigital

- Cigital's Software Security Group invents and delivers Software Quality Management
- WE NEED GREAT PEOPLE
- See the Addison-Wesley Software Security series
- Send e-mail: gem@cigital.com



For more

cigital

"So now, when we face a choice between adding features and resolving security issues, we need to choose security."

-Bill Gates