Software Security: Is OK Good Enough?

Appsec USA 2011
September 22, 2011

John B. Dickson, CISSP
Denim Group, Ltd.
@johnbdickson
OWASP AppSec 2011
OWASP AppSec 2011
OWASP AppSec 2011
Personal Background
Personal Background
OWASP AppSec 2011
Software Security: Is OK Good Enough?

- Current State of Affairs in Software Security
- What we can Learn from Other Justification Models
- Potential Software Security Justification Models
- Questions and Answers
Current State of Affairs in Software Security

- Testing approaches differ wildly
- Incredible amount of energy focused on technical merits and demerits of testing activities
  - Existing application security scanners identify a subset of vulnerabilities in applications
  - 30-40% Coverage level is accepted norm
  - SQL injection/XSS – yes
  - Authorization & business logic – not so much
1996 Network Security Question?
2011 Application Security Question?

I’ve run my Automated SQL Injection & XSS Application Scanner?
Checkbox Culture

• Compliance culture and resource constraints have limited software security coverage
• This cuts to the heart of “OK”
• Heartland Payments Systems breach and PCI test coverage
  – Organizations try to limit PCI audit by design, even if many view PCI DSS as the most rigorous application security compliance framework
Going Concern: In accounting, "going concern" refers to a company's ability to continue functioning as a business entity.
What do Street Vendor food and iTunes applications have in common?
Introduction of malware into iTunes & Droid Apps stores

- Applications submitted to the Apple iTunes AppStore and the Google Android store do not undergo rigorous security testing
- Both application stores do not do "white listing" per se
New York City

- 24,000 restaurants inspected/year
- Point-based rating scale
- 3 Categories of violations
  - Public health hazard (7 points)
  - Critical violation (5 points)
  - General violation (2 points)
Venture a Guess?

- 3 Categories of violations
  - Public health hazard (7 points)
  - Critical violation (5 points)
  - General violation (2 points)
Venture a Guess?

- 3 Categories of violations
  - Public health hazard (7 points)
  - **Critical violation (5 points)**
  - General violation (2 points)
What we can Learn from Other Justification Models – Earthquake Building Codes

Haiti vs. Chile
What we can Learn from Other Justification Models

• What we can learn from these two models?
• No model is based purely on industry-driven compliance
  – Have no regulation is bad
• Starting point is a generally accepted need for regulation
  – Buyers need to demand software “seatbelts”
  – Political consensus in Chile & California to enforce more stringent building codes
• Must have Rule of Law present to enforce regulation
  – Building codes were in place in both Chile & Haiti
• Misguided regulation may be more destructive than no regulation at all
  – e.g., Sarbanes Oxley
So where do you go from here?
Software Security Justification Models in an “OK” World

What can be Done Globally?
We need more Earthquakes
We Need Better Mainstream Scary Stories
We Need Better Mainstream Scary Stories
We Need Smarter buyers
There’s an App for That!
Software Security Justification Models in an “OK” World
- In the World you Influence
Tailor Responses for Limited Resources - ASVS “Applied” Case Study

- Financial Services firm services 2,000 + banks
- Before
  - Reactive testing
  - No repeatable or predictable
  - Poor coverage
- After
  - Acceptable level of security testing
    - Applied 80/20 rule to clients
  - Predictable results
  - Mutually understood results
Tailor Responses for Limited Resources - Open Software Security Maturity Model (OpenSAMM)
Tailor Responses for Limited Resources

Measure, Measure, Measure
Realize that Sales & Marketing is our #1 Job
We Need Better Developers

• Is it enough to say you are “Rugged”
• We need software developers to elevate their coding practices to lower the number of obvious security vulnerabilities
• These developers need better tools
  – Modern frameworks
  – Static analysis baked into build
• Starting point – software engineers need to be further along out of college
• Industry responses
  – Carrot & stick models
The New Negligence: Eliminate SQL Injections and XSS

Sawmill Error: Unexpected end of configuration

; Error occurred at: :/tulip/tulip1/sawmill/v7/production/src/config_node.cpp:1129;

Error occurred while processing pair configuration string:

http://127.0.0.1:8987

vulnerable to XSS

OK
The Negligence: SQL Injections and XSS

XSS & SQL Injections
We need better coverage of attack space
We need better coverage of attack space
We need better coverage of attack space
Questions, Answers, & Contact

John B. Dickson, CISSP
john@denimgroup.com
(210) 572-4400

www.denimgroup.com
blog.denimgroup.com
Twitter: @johnbdickson