Building an Effective Application Security Practice on a Shoestring Budget

John Viega

VP, Chief Security Architect

David Coffey

Manager, Product Security

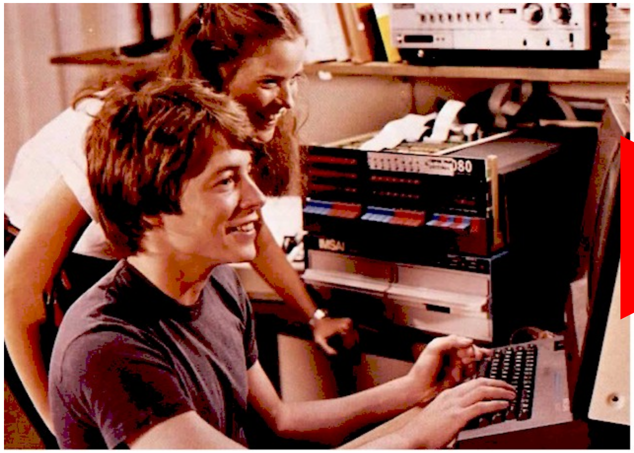
Agenda

- Application Security and understanding the problem
  - Evolution
  - The cost of doing nothing
  - Known issues and regulations
- Finding a solution to the problem
  - Best Practices
  - What works and what other people have implemented
- Showing that the solution works
  - Mantra: “Metrics are your Friend”
  - Measuring the un-measurable
  - Alignment with business goals

What is application security?

- Application security
  - — catch-all phrase for the research, study, and remediation of security problems in applications
- What is the problem?
  - — Bugs in software that may allow for manipulation of the program or computer to lead to un-intended results
- “Why can’t we just fix the problem?”
  - — Complexity
  - — Time
  - — Technology
  - — Knowledge

Evolution of Application Security

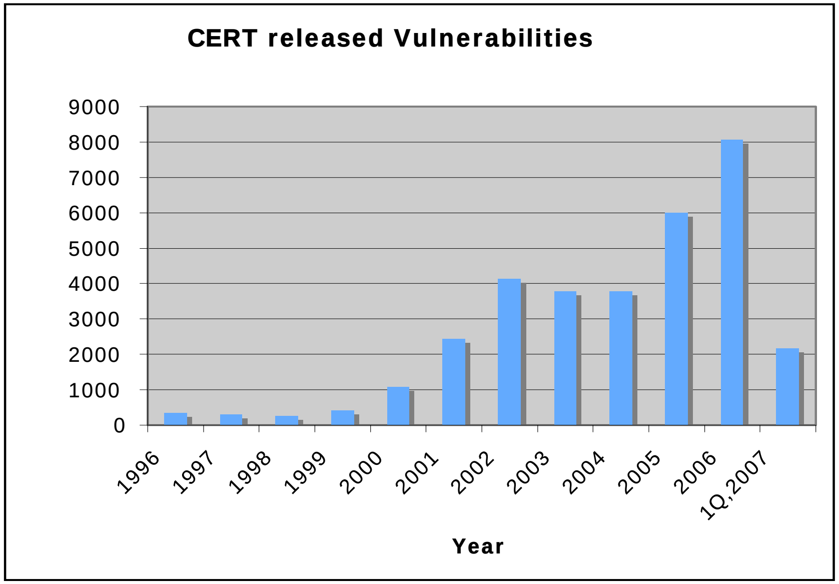


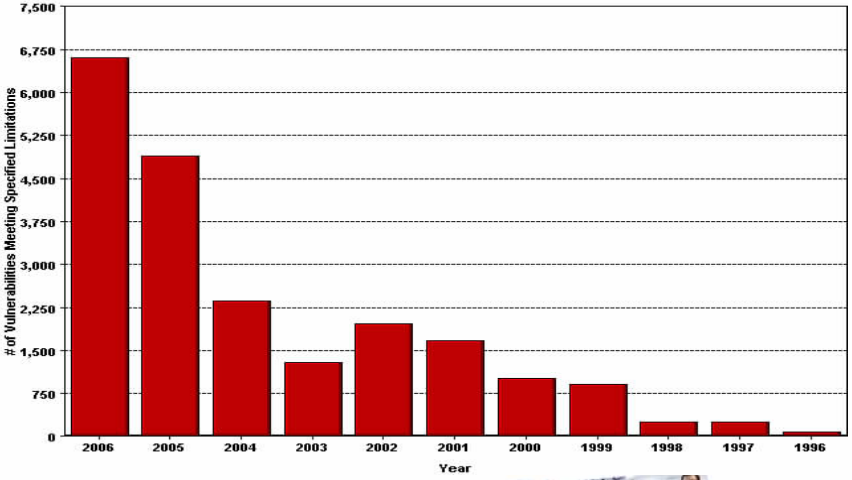
```
       state          service
22/tcp       open           ssh

o exact OS matches for host

map run completed -- 1 IP address (1 host up) scanneds
 sshnuke 10.2.2.2 -rootpw="Z1ON0101"
onnecting to 10.2.2.2:ssh ... successful.
empting to exploit SSHv1 CRC32 ... successful.
seting root password to "Z1ON0101".
stem open: Access Level <9>
sh 10.2.2.2 -l root
t@10.2.2.2's password:
```

- Lowest hanging fruit phenomenon
  - Aided by the internet
  - Progressed from gateway perimeter to host and application
- Functioning as designed?
  - Port 80 is open and 443 is open and not monitored

How bad is it?

- Steadily increasing trend
  - — Due to better knowledge?
  - — Due to more software?
  - — Due to worse software?
  - — Irrelevant!
- This is only the public side
  - — Underground knows of issues months and years before they are released
  - — So do the vendors





-Top graph is generated from CERT data found on http://www.cert.org/stats/

- Bottom grap is generated from the National Vulnerability Database found at http://nvd.nist.gov/

McAfee

Protect what you value.

How many issues get detected?

- According to the FBI 2006 summary report
  - 52% had a break in
  - 10% are clueless
- According to DISA in 1996
  - 65% of attacks are successful
  - 2.6% are detected
- Getting better

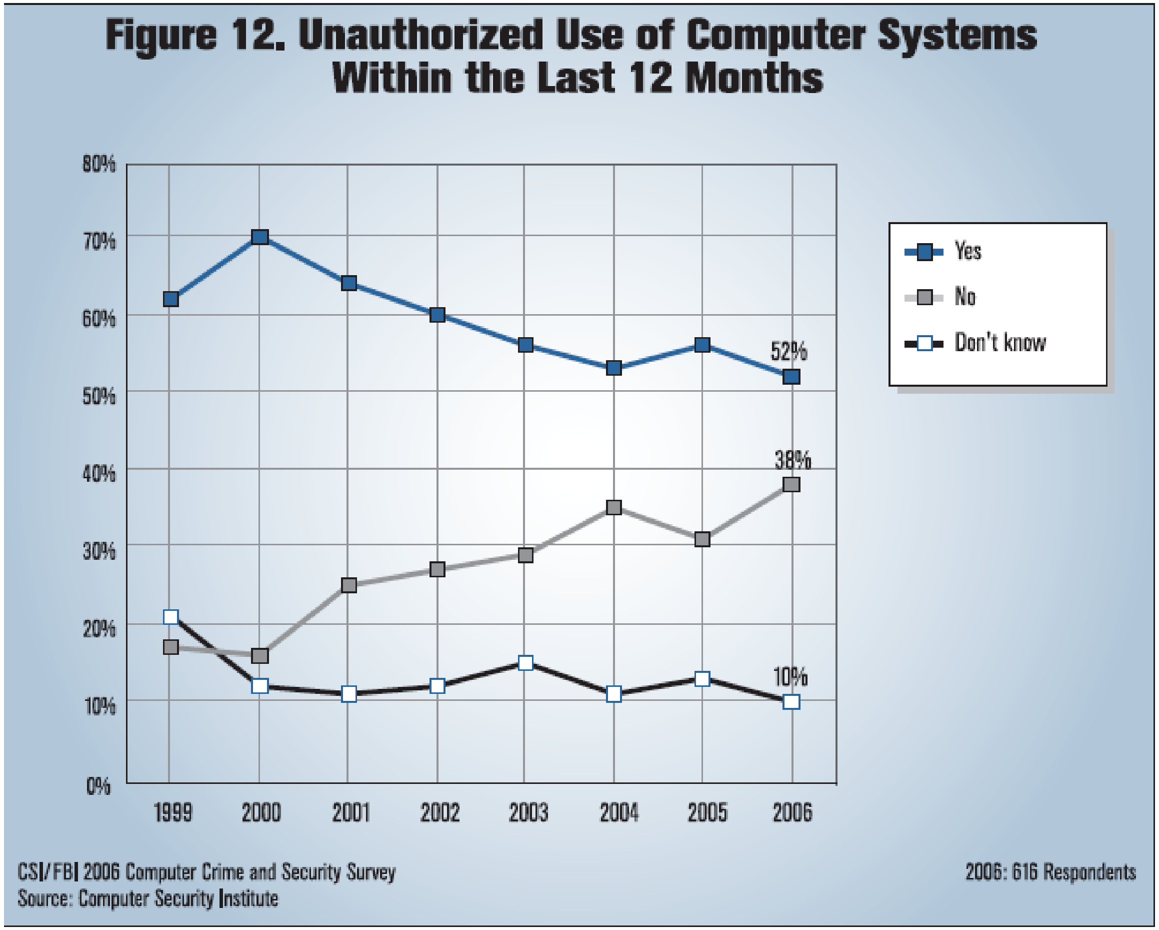


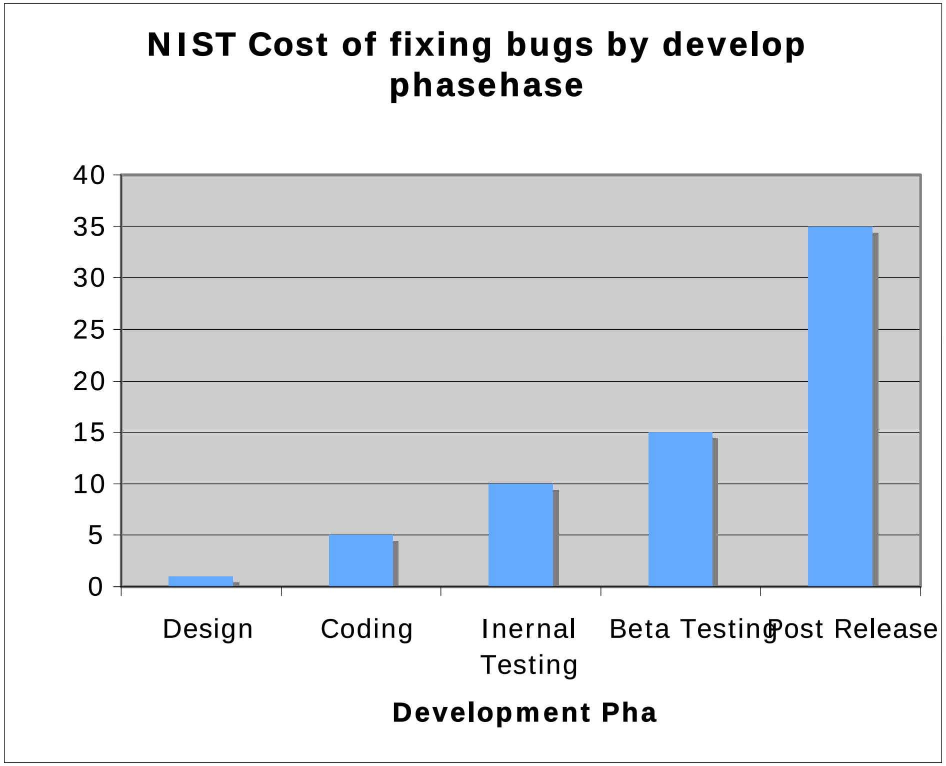
Figure 12. Unauthorized Use of Computer Systems Within the Last 12 Months

CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

How much does it really cost to fix a bug?

- Cost to fix bugs is exponential per development phase
- Coupled with the exponential vulnerability release
  - — Hurts business
  - — Hurts schedules
  - — Hurts efficiency
- Business driver for adding security early on



Hidden Cost of insecure solutions

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

- In 2005, study shows that average stock price drops .63%
- Highest price drop McAfee has had is $.32 or <1%

Impact of Software Vulnerability Announcments on the Market Value of Software Vendors - an Empirical Investigation by Rahul Telang and Sunil Wattal

PR and Customer Cost

- Vulnerabilities represent a Public Relations nightmare
  - Customers feel betrayed
  - Partners not responsible but held accountable
  - How do you defend the accusation that the computer is safer without your software on it?

Types of Finders

- Internal
  - Employee of the company
  - Hired security firm
- External
  - Security researcher
  - Partner
  - Knowledgeable end-user
- Hostile
  - Malware or targetted attack

Internal Finders

- Developer, architect, QA, hired security hand
- Usually can be trust worthy
  - it is their job
  - contracts
- Has several motivations
  - Curiosity
  - Prestige
  - Mission
  - Job

External Security Researcher

- Someone who finds security flaws in applications
- Unknown trust level
  - They will usually communicate their intentions
- Has several motivations
  - Money
  - Prestige
  - Curiosity
  - Mission
  - Malice

McAfee

Protect what you value.

External Partner or Customer

- Business partner who is exposed to more IP
- Usually can be trustworthy
  - — You are in business together
  - — May not understand the full implications
- Has several motivations
  - — Risk Assessment
  - — Business improvement
  - — Customer acquisition
  - — Curiosity

Hostile Attacker and Black Market

- Someone who needs to exploit for a reason
- Completely un-trustworthy
  - They have full knowledge of what they are doing
  - Only one reason to do it
- Has several motivations
  - Money
  - Political or personal motivations
  - Prestige

What we know about the Black Market

- Increasingly being run by organized crime
  - Recruiting people out of college like agencies
  - Very adept at running a business
- Pay out well for vulnerabilities
  - Going rate of IIS6 is in the 7 figures
  - Fresh IE flaws in the tens of thousands
- Continually need fresh exploits
  - Once they are patched == useless
  - Need cheap ways to re-use old methods
  - Highly specialized

Regulations, Standards, oh-my!

- Information Security is growing up!
  - And has to deal with the pains
- New laws and standards have been established
  - Sarbanes Oxley Act (SOX)
  - Gramm-Leach-Blily Act (GLBA)
  - HIPPA
  - EU Privacy
  - ISO 17799:2005
  - Visa PCI
- Rome was not built in a day
  - They may not be perfect, but need to start somewhere

Sarbanes-Oxley Act of 2002 (SOX)

- Purpose? Prevent Corporate Fraud
- How? Holds the executives of the company personally accountable for the accuracy of their data
- Is this effective? Hell yeah!
- Punishment?
  - Fines
  - Serve time
- Why was it created?
  - Response to a string of corporate fraud cases like Tyco and Enron

Security and SOX

- The Act is huge, what sections do I need to worry about?
  - — 302:Corporate Responsibility for Financial Reports
    - Outlines who is responsible for what
    - Outlines that adequate controls need to be established
      - — Maintain confidentiality and integrity of data
      - — Maintain accountability
  - — 404:Management Assessment of Internal Controls
    - Outlines that controls need to be managed properly
    - Requires a yearly audit on established controls
  - — 409:Real Time Issuer Disclosures
    - Requires the company to disclose “in a rapid and current basis” anything that the public will need to know in order to “protect investments”
  - — CONSULT YOUR LAWYER!!!

How does SOX affect application security?

- Remember basic security principles (CIA + AAA)
  - Log files
  - Strong password policies
  - Secure network communication
  - Secure backup and storage
  - Session management
  - Vulnerabilities which may circumvent these
- Know who you are selling to and what it is used for
  - Several of our products have to go through a SOX compliant requirements review

Financial Modernization Act of 1999 (Gramm-Leach-Blily Act or GLBA)

- Purpose? Prevent identity theft and crimes
- How? Placed controls around financial data
  - What data can be collected
  - What and how that data can be stored
  - What and how that data can be disclosed and shared
- Is this effective? Moderately
  - Still some loopholes in place to allow business to function like subsidiaries
- Punishment?
  - Fines
- Why was it created?
  - Allow financial mergers and stop the ease in which data is stolen
  - Victoria’s Secret???

GLBA side story

- So the story goes…
- Title V (consumer data privacy) proposed by Ed Markey (D-MA)
  - Opposed by financial companies (no kidding)
  - Originally opposed by others including Joe Barton (R-TX)
- Until, Joe started receiving Victoria's Secret catalog
  - His personal information had been sold by his bank
  - Had to answer a few questions to his wife (addressed to him)
  - He changed his support
    - Apparently politicians don't have too many personal problems with their data being sold off

Security and GLBA

- What sections to worry about
  - TitleV: Privacy
    - Section 501: Protection of Nonpublic Personal Information
      - Ensure confidentiality and integrity of personal information
    - Section 502: Obligations with Respect to Disclosure of Personal Information
      - Ensure proper disclosure is followed and customer is alerted
      - Always allows for an “opt-out”
    - Section 521: Privacy Protection of Customer Information for Financial Institutions
      - Stops “pretexting”
      - Makes fraudulent requests for information ilegal (social engineering)

How does GLBA affect application security?

- Openly depends on the security of the systems
  - Outside the scope of the act
- Need to worry about how financial data is:
  - Stored
  - Backed up
  - Logged
  - Transferred
- Affects all “financial institutions”
  - Be prepared for customer questions and new features

ISO/IEC 17799:2005

- Purpose? Provide an international code of practice for information security management
- How? Provides a series of best practices
  - Covers everything from physical to application security
- Is this effective? Moderately
  - Not the end-all reference people believe it is
  - Needs supporting documentation
- Punishment?
  - none
- Why was it created?
  - Effort to create an international security management standard
  - Original edition contained the City of London fire code

Application Security and the 17799:2005

- What sections to pay attention to
  - Section 10: Communications and Operations Management
    - Protection against malicious and mobile code
    - Security of network services
    - Audit logging
  - Section 11: Access Control
    - Application and information access control
  - Section 12: Information Systems Acquisition, Development, and Maintenance
    - Cryptographic controls
    - Security in development and support processes
  - Section 13: Information Security Incident Management
    - Reporting and management of security events, weaknesses, and incidents
  - Section 15: Compliance
    - Legal requirements and audit considerations

Application Security and the 17799:2005

- What it is not
  - A specific HOWTO detailing exactly what must be done
  - A legal document
- What it is
  - A set of best practices and guidelines to follow when doing one of the above
  - Example: outsourcing development, what to do?
    - Go to section 12.5.5 and read the list of things you need to take care of
      - IP rights and laws
      - Oversight
      - Contracts for quality and accuracy
      - Ability to conduct audits
      - Etc.
  - More like a shopping list or Chinese take-out menu

Visa Payment Card Industry Data Security Standard (PCI DSS or just PCI)

- Purpose? Prevent identity theft and fraud
- How? Placed controls around card data and merchant sites
  - What data can be collected and how it can be stored
  - How secure online merchant sites should be
- Is this effective? Moderately
  - Only scanned quarterly
  - Scanning vendors need to qualify annually with VISA
- Punishment?
  - Become non-compliant
- Why was it created?
  - Gesture of making online merchants more secure for customers

Application Security and PCI

- Which sections to pay attention to
  - — Requirement 3+4: Protect Cardholder Data (rest/transmission)
    - Encrypting data while at rest and in motion
    - Ensure confidentiality and integrity of data
  - — Requirement 6: Develop and Maintain Secure Applications
    - Must be free of common security flaws
    - OWASP top 10 (input validation…)
  - — Requirement 7-9: Strong Access Controls
    - Best practices around access controls
  - — Requirement 10+11: Regularly Monitor and Test
    - Must do a quarterly test and review
  - — Requirement 12: Maintain a Security Policy
    - Have a plan for remediation and incident management

Application Security and PCI

- Encryption
  - Use standard libraries, DO NOT BUILD YOUR OWN!
- OWASP top 10
  - Mostly centers around input validation
    - Injection, XSS, overflows, etc.
  - Improper error handling and others
  - http://www.owasp.org/index.php/Top_10_2007

Best practices overview

1. Institute security awareness programs
2. Establish and monitor security metrics
3. Document security-relevant requirements
4. Apply security principles to design
5. Perform security analysis of requirements and design
6. Research and assess security posture of third-party software
7. Perform source-level security review
8. Identify, implement and perform security tests
9. Build operational security guide
10. Check operational security configuration

Institute security awareness

- Why security awareness training?
  - People need focused education in order to build security in
  - This can have the largest impact of all the best practices
- Program should target everyone involved
  - Product and Project Managers
  - Requirements Specifiers
  - Architects & Designers
  - Developers
  - Testers
  - Help Desk
- Program should be aligned with the technical standards and controls supporting established information security policies (e.g. coding standards)
- Program should stress accountability

Security Metrics

- Overcoming “security is a cost” mentality
  - It is possible to show a Return on Security Investment (ROSI)
  - If studies can show the usefulness of security, so can you
- Overcoming “security geek” label
  - Metrics are the “universal language” of business, use it
  - Suits might not know what a “double free” is, but they do understand saving the company 7 figure risk from attacks
- Getting the bigger budget, headcount, cool projects
  - Showing effectiveness and usefulness allows growth
- Alignment with business goals
  - If they understand, security can be more useful to the company

Establish and monitor metrics

- Why security metrics are important
  - Risk management
  - Measurement of effectiveness
  - Accountability
  - Guidance on compensating controls
  - Alignment with business goals
  - Compliance and regulation
  - Audits and emergency situations

Metrics should be SMART+

- Might have been around for a while, but it is true

- S - Specific
- M - Measurable
- A - Attainable
- R - Realistic
- T - Traceable
- + - Appropriate

How do you measure the un-measurable?

- How do you measure the security of an application?
  - You can measure the progress of securing it
  - You can use lessons from quantum physics and measure the effect on the environment
- It is impossible to prove that something is secure
  - Need to show that you are making progress
  - Raising the bar makes things less attractive to attackers

What should the goals be?

- The application is becoming more secure
- Developers are writing better code
- Fewer and less severe reports are coming in
- Compliance and regulations are being met
- Business goals can be established and are being met
- Deliver clear and concise timely reports to business

Showing the application is more secure

- Things that are known
  - Lines of code
  - Bugs found in code ranked by severity, probability, CVSS
  - Types of bugs found
  - How long it takes to fix the issues
  - Reported issues from customers, partners, researchers
  - Tracking these numbers over time
- What can you do with this?
  - Average defect density broken up by project, bug type, severity, and being tracked over time
- What this shows
  - How secure the application is becoming
  - Trends in fixing what type of issues and how long they take
  - Trends in classes of vulnerabilities within the organization

Showing developers are writing better code

- Things you know
  - Lines of code added by which developer
  - Which internal courses have been attended and when
  - Defects added per line of code, severity, and type (automation is your friend)
  - When audit has been completed and how many issues belong to which developer
- What can you do with this?
  - Compute errors added per line of code over time against events in time
- What this shows
  - How developer improves over time
  - How courses affect developer’s quality of code
  - How security audits affect developer’s quality of code

Showing fewer and less severe reports being made

- Things you know
  - Issues being reported in rated by type, severity
  - Issues being reported in by who
  - When audits have been completed and which bugs fixed
- What can you do with this?
  - Compute issues being reported in by who, organized by project, severity, and compared against the audits
- What this shows
  - How issues found in audit compare against issues found from researchers (are you finding what you should be finding)
  - How this occurs over time, by project and bug type
  - How long it takes to research, respond, and remediate

Compliance and regulation

- Work closely with the auditors to
  - Establish scope
  - Determine what is lacking and what is good
  - Establish a plan to reach acceptance
- Integrate with QA
  - Establish what your product needs to be compliant with
  - Create a testing plan to show compliance
  - Integrate tests with QA to test for compliance on every release if possible
- Check up on a regular basis
  - Notice deviations
  - Review any changes in regulation or standards and how that affects your standing and current tests

Protect what you value.

Delivering timely and clear reports

- Work with other business groups to see what they do
  - Probably already established
  - Fit in with their schedule and format if possible
- Programs like Six Sigma work well
  - Establish goals on a quarterly basis
  - Establish what metrics others should be tracking
  - Create an integrated score card
- Rome was not built in a day
  - It takes time to get it right
  - Trends are going to whacky for a while as well
  - It will show results faster than you think

Conclusion

- Understanding what threats are out there
  - Where they come from
  - How to face them and expectations for the future
  - How laws and regulations need to be accounted for in projects
- Understanding best practices
  - What is out there
  - Established processes for over 6 years
- Understanding how to show progress
  - Leveraging what you know to do a better job
  - Proving things are getting better
  - Aligning with business goals

Questions?