Auditing Application Security

Todd McCavit, Director
Protiviti

September 13, 20112

Agenda

- Why application security auditing matters
- Keys to a better application security audit
- Additional application security topics
- The castle analogy
- Questions

Why Application security auditing matters

Why Application Security Auditing Matters

Largest Data Security Breaches

1. Heartland Payment Systems

Date: March 2008

Impact: 134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.

2. TJX Companies Inc.

Date: December 2006

Impact: 94 million credit cards exposed.

3. Epsilon

Date: March 2011

Impact: Exposed names and e-mails of millions of customers stored in more than 108 retail stores plus several huge financial firms like CitiGroup Inc. and the non-profit educational organization, College Board.

Source: CSOONLINE : http://www.csoonline.com/

Why Application Security Auditing Matters

Latest News and Trends

Office of the U.S. Trade Representative (USTR) tabulates the cost of intellectual property theft at about $250 billion annually to American businesses and citizens. This number is growing and represents the theft of key technologies and the hard-learned processes that help turn them into products.

Pop Quiz: Who is the Ambassador of the USTR?

Why Application Security Auditing Matters

Latest News and Trends

The Identity Theft Resource Center tracks data-breach incidents and the number of exposed records related to payment cards, customer, university or patient data when that's known. Here are the Top 15 Worst so far for 2012 based on number of exposed records — and the year's only half over.

Source: http://www.networkworld.com/slideshow/52525#slide1

Why Application Security Auditing Matters

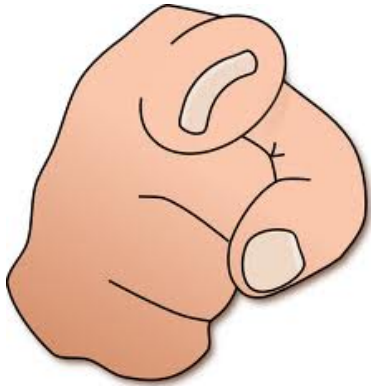
Latest News and Trends

- In November 2011, 14 U.S. intelligence agencies issued a report describing a far-reaching industrial espionage campaign by Chinese spy agencies.
- The campaign targeted a swath of industries: biotechnology, telecommunications, and nanotechnology, as well as clean energy.
- One U.S. metallurgical company lost technology to China's hackers that cost $1 billion and 20 years to develop, U.S. officials said last year

Source: http://www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage#p2

Why Application Security Auditing Matters

Importance of Auditing App Security



- Your job of auditing application security is important!
- You are independent and can challenge the status quo

Keys to a Better Application Security Audit

- **Proper planning**
- **Review the skills, knowledge, and effectiveness of the IT team**
- **Go beyond basic control based auditing**
- **Use automated tools**
- **Talk to people**
- **Use Subject Matter Experts**
- **Remain skeptical**
- **Challenge the status quo**

Keys to a Better Application Security Audit

Proper Planning: Understand the Objectives

- The first thing you have to understand is what are the objectives of the audit.
  - Why is the audit being performed?
  - Who is asking for the audit?
  - Are there expectations on how the audit will be executed?
  - What is the timing of the audit?

Keys to a Better Application Security Audit

Proper Planning: Understand the Objectives

- To be ***truly*** effective in auditing application security you have to first understand the **type of risks** with the application being used and the **significance of those risks**. This understanding allows the auditor to design the **appropriate type of tests**.

Keys to a Better Application Security Audit

Proper Planning: Know the Data

- High Risk Data
  - Personally Identifiable Information
  - Credit card data
  - Medical information
  - Intellectual property
  - Financial information
- Data Governance initiatives in place

Keys to a Better Application Security Audit

Review IT Team: The Security Administrator

- Key line of defense
- Should not be just a machine that only does what he is told
- Should take ownership of the Security
- Should be willing to challenge things that don't make sense

Keys to a Better Application Security Audit

Review IT Team: The Developer

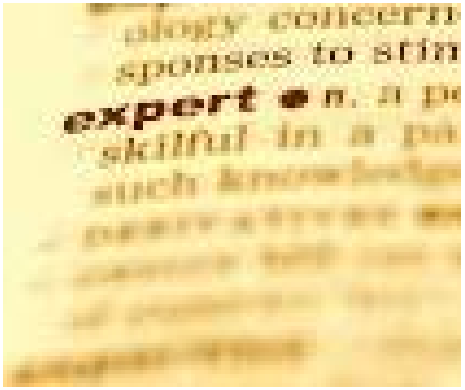
Often times developers do not have security at the core of their belief system.

Speed
Reliability
Accuracy
Creativity

are often traits that are rewarded in revered in developers but **NOT ALWAYS SECURITY!**

Keys to a Better Application Security Audit

Use Subject Matter Experts



- Challenge of staying on top of all aspects of IT is impossible.
- Ability to challenge status quo is much easier
- Can be used to help plan and develop recommendations
- Importance of networking

Keys to a Better Application Security Audit

Use Automated Tools

- Scope coverage is increased dramatically
- Another form of SME
- Reduces cost
- Reliability increases
- Must know the data required

Keys to a Better Application Security Audit

Beyond Basic Control Auditing:

Challenge Access Review Effectiveness

- Size of the report
- Amount of detail
- Is the resource trained on the report/security?
- Do changes result from the review?
- Frequency/Timeliness

Keys to a Better Application Security Audit

Talk to People

- Often overlooked in an IT audit
- Talk to a variety of people
- Talk to the business
  - They have a unique perspective
  - More willing to disclose issues in the security process
  - Potential to support recommendations for improvement

Keys to a Better Application Security Audit

Remain Skeptical and Challenge the Status Quo

- "We've always done it this way"
- Verify as much as possible
- Use SME's, Automated Tools, Benchmarking
- Must be done with the right attitude and tone

Other Application Security Topics

2 Factor Authentication

- Becoming more mainstream
- Should be considered for higher risk systems
- Level of control is much higher than just passwords

- Consider for a subset of users (admins, key power users, etc as a pilot)

Other Application Security Topics

Custom Developed Applications or Code

- Use developers as part of your audit team – Look for loop holes or inconsistency in coding – must be specific on what they are looking for
- Database Links – Look for places in the code where application is being granted full access to databases
- Code Quality Standards
- Code Review process

Other Application Security Topics

Segregation of Duties

- Can be a very large effort if done at a detailed level
- The importance of the ruleset
  - Sufficiency of the ruleset
  - How is it maintained…when was the last update?
- Make sure and check the on mitigating controls
- Make sure to factor in time to look for false positives
- Will need time with process owners

Other Application Security Topics

User ID's and passwords

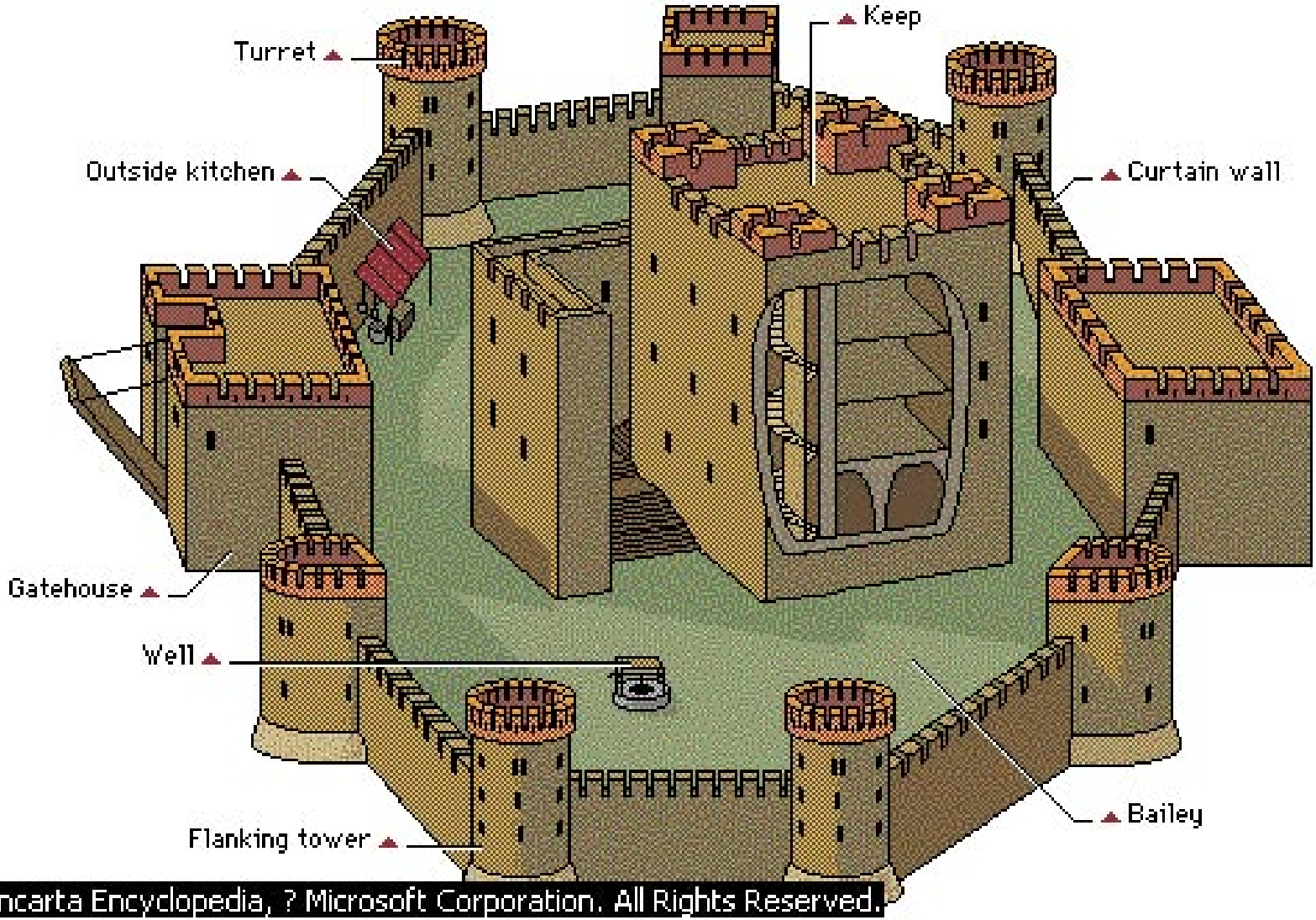
- Generic passwords
- Password resets
- The role of the help desk
- Application won't allow for password controls

Other Application Security Topics

Logging

- Often not used…As IT Audit we should make and see if that is appropriate
- Memory is so cheap that this excuse is not as valid as it used to be
- Use of tools allows for analysis of Logging
- Application won't allow for password controls

Security as a Castle



Anatomy of a Castle

- Moat =the network layer
- Walls and draw bridge = User ID's and passwords
- The tower = Monitoring
- The security Camera ? = Logging
- Infirmary = Help Desk