Agenda

- Security Problems and Statistics
- Analysis
- Strategic Planning
- Conclusion
Yen-Ming Chen

- Director of Consulting, Northwest.
- Joined Foundstone in 2000
- 4 Contributing authorships: HE 3rd edition, HE of Web App, Win XP professional Security and HackNote Web security
- Dozens of articles in SecurityFocus, DevX, SysAdmin, PCWeek, CNET Taiwan, ITHome and other medias
- Invited speaker for world wide security conferences
Thus do many calculations lead to victory, and few calculations to defeat

SECURITY PROBLEMS
Current Status

- Security Maturity
- Attack Target Shift
- Security Ecosystem
- SQL Injection
- Why You Still Can’t Rely on Automated Tools
Information Security Maturity: 1996

Blissful Ignorance
- Review Status Quo
- (Rer) Establish Security Team

Awareness Phase
- Develop New Policy Set

Corrective Phase
- Institute Processes
- Initiate Strategic Program
- Design Architecture
- Conclude Catch-Up Projects

Operations Excellence Phase
- Continuous Process Improvement
- Track Technology and Business Change

NOTE: Population distributions represent typical, large G2000-type organizations
Information Security Maturity: 2000

- Blissful Ignorance
  - 60%
  - Review Status Quo

- Awareness Phase
  - 28%
  - Develop New Policy Set

- Corrective Phase
  - 10%
  - Institute Processes
  - Conclude Catch-Up Projects
  - Design Architecture

- Operations Excellence Phase
  - 2%
  - Continuous Process Improvement
  - Track Technology and Business Change

NOTE: Population distributions represent typical, large G2000-type organizations
Information Security Maturity: 2004

Blissful Ignorance Phase:
- Review Status Quo
- (Re-) Establish Security Team

Awareness Phase:
- Develop New Policy Set
- Design Architecture
- Institute Processes

Corrective Phase:
- Conclude Catch-Up Projects
- Institute Processes
- Initiate Strategic Program

Operations Excellence Phase:
- 5% Continuous Process Improvement
- Track Technology and Business Change

NOTE: Population distributions represent typical, large G2000-type organizations
Information Security Maturity: 2008

- Blissful Ignorance
- Awareness Phase
- Corrective Phase
- Operations Excellence Phase

Duration 3+ years

- Review Status Quo
- Develop New Policy Set
- (Re-)Establish Security Team
- Conclude Catch-Up Projects
- Design Architecture
- Institute Processes
- Initiate Strategic Program
- Track Technology and Business Change

Continuous Process Improvement

Maturity
Attack Target Shift

- From server to application; from corporate network to every user.
Google Search Trend

**Search Volume Index**

- **sql injection**: 1.00
- **buffer overflow**: 0.58
- **cross-site scripting**: 0.02
- **csrf**: 0.03

**News reference volume**

- 2004
- 2005
- 2006
- 2007
- 2008

OWASP
SQL Injection

- RFP (Rain Forest Puppy) identified the problem in Phrack 54 (December 1998)
  - http://www.phrack.org/issues.html?issue=54&id=8#article
- In 2005, Cardsystem lost 40 million credit card info
- In 2008, an automated mass attack of 500,000 (estimated) web servers
  - Yes, using SQL Injection!
- Exploits of a mom (http://xkcd.com/327/):

  ![Exploits of a mom](image)
Why You Still Can’t Rely on Automated Tools?

- North Carolina News 13
- Web-based “closings” ticker for schools/businesses

Submit info → Human approval → Stack messages → TV

http://tinyurl.com/pwpec
This is What You See...
UAL vs. Google

An old article about UAL's 2002 bankruptcy-court filing resurfaced Sep 8, 2008 as an apparently fresh report on Google's news service. Stock in the parent company of United Airlines quickly dropped to $3 a share from nearly $12.50 before the Nasdaq Stock Market halted trading and UAL issued a statement denying any fresh Chapter 11 filing.

UAL's stock price ended Tuesday's session at $10.60, ...
UAL vs. Google

Sep 6, 2008 10:36pm PDT, A new link to the UAL story was found

Sep 8, 2008 UAL stocks dropped from $12 to $3

$1.1 Billion market value disappeared in a few hours!!!

Google news took and indexed the link
Some Survey Data

Figure 20. Techniques Used to Evaluate Effectiveness of Security Technology
By Percent of Respondents

- Security audits by internal staff: 63%
- Penetration testing by internal staff: 53%
- Security audits by external organization: 53%
- Automated tools: 49%
- Web activity monitoring software: 45%
- E-mail monitoring software: 44%
- None: 12%

CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 475 Respondents
McGraw Touchpoint Secure SDLC
Microsoft SDL

Requirements
- Security Kick Off
- Register with SWI

Design
- Security Design BP
- Threat Modeling

Implementation
- Secure Development Tools
- Best Practice
- Security Documentation and Tools

Support
- Security Servicing
- Security Response

Verification
- Security Push
- Security Testing

Release
Where are things going?

- Penetration testing is still how a lot of companies are going to assess their security.

- Frameworks/libraries/etc are going to make shooting yourself in the foot harder (xss, SQLi, etc).

- “Silver Bullet” devices/technologies are always going to be around.

- SDL is starting to show proven results.
What’s Next?

■ Security research is chasing after new technologies
  ▸ New vulns on different products will happen daily
  ▸ Better accuracies from security products
  ▸ Slower to see new paradigm shift

■ Integrate security into your daily life
  ▸ Corporate M&A
  ▸ Need better management on execution
  ▸ New technologies to make it harder to make unsecure web applications

■ Learn from other fields
  ▸ Knowledge Discovery, Data Mining & Information Retrieval
  ▸ Biology, Physics, Social Science and others
Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight

WEB APPLICATION SECURITY
2007-2008 Analysis

- Collected 77 Applications in 5 industries
- Picked 27 out of them and did further study
- Arranged findings based on
  - Foundstone Security Framework,
  - Overall risk level and
  - Root cause in SDLC phases
Foundstone Security Framework

Configuration Management
- Secure deployment and hardening. Issues will include default deployment settings and administrative access

Data Protection
- Handling of sensitive data as it is at rest in files and databases or as it is transmitted across the network

Authentication & Authorization
- Access to protected resources and kinds of controls on such access. How identities are verified.

Logging & Auditing
- What information is logged and where it is logged. Can information act as audit trail?

Data Validation and Exception Management
- How the application performed data validation on both input and output and how exceptions are being handled without information leakage
Financial Services - 15 Apps
Healthcare - 12 Apps
Insurance - 27 Apps

Diagram showing the radar chart with the following categories:
- Authentication
- Authorization
- Configuration Management
- Error Handling
- Discovery
- Data protection
- Data Validation
- User and session management

The diagram highlights the Industry sector with a red area.
Retail - 17 Apps

Diagram showing the following categories:
- Authentication
- Authorization
- Error Handling
- Configuration Management
- Data Protection
- Data Validation
- User and Session Management

Industry key highlighted in red.
Utility - 6 Apps
27 Applications

- 13 on Unix; 13 on Windows; 1 on Novell
- Total 421 findings
Findings by Framework and Risk Level
High and Medium Risk Findings
Findings by Percentage
Findings by SDLC Phases
White Box vs. Black Box

White Box vs. Black Box Testing: Issues Discovered by Foundstone in 2005-2006

- White Box (Threat Modeling & Code Review)
- Black Box (Penetration Testing)

Issues:
- Configuration Management
- Data Protection in Storage & Transit
- Authentication
- Authorization
- User & Session Management
- Data Validation
- Error Handling & Exception Management
- Logging & Auditing

Percentages:
- Configuration Management: 21.43%
- Data Protection in Storage & Transit: 14.72%
- Authentication: 14.29%
- Authorization: 23.06%
- User & Session Management: 17.22%
- Data Validation: 32.86%
- Error Handling & Exception Management: 16.11%
- Logging & Auditing: 10.71%
- Total Unknown: 13.89%
10 Things To Secure Your Web App

- **Authentication**
  - Password policy
    - Reset password function, history, complexity and account lockout

- **Authorization**
  - Role/privilege mapping and enforcement
  - Workflow/business logic authorization enforcement

- **Data Validation**
  - Do your validation on the server-side both on output and input!

- **Session Management**
  - Use random session ID and maintain the state on server-side. Do not depend on any state information on the client

- **Data Protection**
  - Protect your important data in storage and transit
  - Choose your data protection solution wisely

- **Configuration Management**
  - Secure server configuration and patch it well!

- **Exception Management**
  - Handle all exception and return generic error messages

- **Logging and Auditing**
  - What to log and how/when to audit?
If you know the enemy and know yourself, you need not fear the result of a hundred battles

STRATEGIC PLANNING
Six Sigma Tactical Steps

- Define
- Measure
- Analyze
- Improve
- Control
What is Process Sigma?

- Defects per Unit and Opportunities

- 3.4 defects per 1 million opportunities is Six Sigma

\[
\frac{\text{Number of Defects}}{\text{Number of units} \times \text{Number of opps.}} \times 1,000,000
\]
Balanced Scorecard

FINANCIAL
To succeed financially, how should we appear to our shareholders?

CUSTOMER
To achieve our vision, how should we appear to our customers?

INTERNAL BUSINESS PROCESS
To satisfy our shareholders and customers, what business processes must we excel at?

LEARNING AND GROWTH
To achieve our vision, how will we sustain our ability to change and improve?

VISION AND STRATEGY
Methodology

- Authentication & Authorization
- Data Validation & Exception Management
- Data Protection
- Logging and Auditing

- Requirements
- Design
- Implementation
- Verification
- Release
- Support

- People
- Process
- Technology

- Objectives
- Measurements
- Targets
- Initiatives
Solution

Requirements:
- Regulation
- Policy
- Business requirements
- Known Best Practice

Design:
- Policy
- Specification

Implementation:
- Coding Guideline Standard
- Technology

Verification:
- Test Plan
- Test Methodology
- Tools

Release:
- Hardening guidelines
- Best Practice
- Tools

Support:
- Response Plan
- Security Knowledge Portal
<table>
<thead>
<tr>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Organization</td>
<td>- Policy</td>
<td>- Tools</td>
</tr>
<tr>
<td>- Training</td>
<td>- Guidelines</td>
<td>- Knowledge Repository</td>
</tr>
<tr>
<td>- Budget</td>
<td>- Standards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Best Practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Methodology</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Response</td>
<td></td>
</tr>
</tbody>
</table>
Action Items

Objectives
- Create/enhance secure coding standard
- Train developers to do threat modeling
- Improve security quality from customer’s perspective

Measurements
- Number of implementation bugs
- Number of threats identified
- Number of maintenance patches per month

Targets
- Maintain six sigma
- Every developer should be able to perform 1 TM/year
- Reduce to 2 per month

Initiatives
- Improve current coding guideline/standard
- Computer based training
- Security knowledge management
In order to carry out an attack, we must have means available

CONCLUSION
Summary

■ We reviewed:
  ▸ Current security status
  ▸ Web application security statistics
  ▸ Strategic planning to keep your web application secure

■ Security is an on-going process that also requires people and technology to play important roles.
No Silver Bullets or Easy Button!
If Toyota Builds Your Web Applications...

- Modularization, Automation and Just-In-Time
- Reduce cost, maintain highest customer satisfaction
- Implementation phase will be automated and modularized
- Developers won’t be able to use any insecure implementation techniques
- Web applications will be stick to the known best practice with high quality in security. When there is a serious flaw there will be a recall.
Thank You

Yen-Ming Chen
Director of Consulting,
Foundstone, A Division of McAfee
Yen-ming.chen@foundstone.com