Source Code Protection: Evaluating Source Code Security

Stephanie Woiciechowsk, GSEC
Principal Software Engineer
Product Security Office
EMC Corporation
Goals

• Understand application of basic security concepts
• Collaborative security
• Iterative security improvements around source code

If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them.

-- Thoreau
Why should we care?

Threats to source code
“Consider that no organization is impenetrable. Assume that your organization might already be compromised and go from there.”

Security for Business Innovation Council (2011)

Security takes a new role in working with source code.
Source Code Threats

AMSC Taking Sinovel Infringement Suit to China’s Supreme Court

Ex-NASA contractor arrested on plane to China

-- Bloomberg

Claims by Anonymous about Symantec

--Symantec

- Theft of product-related intellectual property to undermine the security of our customers.
  - Or to seek competitive advantage
- Exposure of vulnerabilities
- Exposure of trade/government secrets

Security takes a new role in working with source code.

-- Symantec
Source Code Threats

AMSC Taking Sinovel Infringement Suit to China’s Supreme Court -- Bloomberg

Ex-NASA contractor arrested on plane to China -- Associated Press

• Theft of product-related intellectual property to undermine the security of our customers.
  • Or to seek competitive advantage

• Exposure of vulnerabilities
• Exposure of trade/government secrets

Claims by Anonymous about Symantec -- Symantec

Security takes a new role in working with source code.
Source Code Threats

- Insertion of malicious code into products during development cycle that can undermine product integrity and operations in customer environments.

Security takes a new role in working with source code.
What can we do?

Define objective
What can we do?

Improve security in the source code environment to defend against threats.

- **Prerequisites & Assumptions**
  - IT is doing their part for corporate security
  - Security is not #1 for SCM, Build, Release, QE, and Dev
  - Security goals often support SCM goals of traceability, reproducibility, and auditability

- **Approach: Collaboration**
  - Define security criteria
  - Understand current environment
    - Review tools in use against criteria
    - Include input from SCM and security experts
  - Manage change
    - Provide recommendations for preferred solutions
    - Provide a framework to assess implementations & evaluate new solutions
Establish Goals & Team

- Initial Goals: Call to action
- Who should be involved?
- Policies & Standards
- Procedures & Assessments

Threat model: How might your environment be attacked?

- Business case
  - What could happen if your source code is modified?
  - What could happen if your source code is stolen?
  - How would you recover and at what cost?

Measureable:
  - Evaluation if a control is in place and how it is functioning

Achievable & Maintainable:
  - Consistent approach to implementation

Policies & Standards

- Source code systems are integrated with organization's identity management system and use network password.
- Transactions are logged to syslog and exported every 20 minutes to a log aggregation system.

RISK REDUCTION

- Establish Goals & Team
  - Initial Goals: Call to action
  - Who should be involved?
  - Policies & Standards
  - Procedures & Assessments

Evaluation:
  - How to implement source code systems?
  - Security: How to modify source code systems?

Reasonable:
  - It is cost-effective to manage security.

RISK REDUCTION

IT Security

Source Code Admin

Legal

Development
Establish Goals & Team

• Initial Goals: Call to action

• Threat model: How might your environment be attacked?
• Business case
  • What could happen if your source code is modified?
  • What could happen if your source code is stolen?
  • How would you recover and at what cost?
• Actionable intelligence

RISK REDUCTION
Establish Goals & Team

- Initial Goals: Call to action
- Who should be involved?
Establish Goals & Team

- **Initial Goals: Call to action**
- **Who should be involved?**
- **Policies & Standards**

  - **Policy:** *What* needs to be done to protect source code.
    - Strong passwords to access source code
    - Transactions will be logged and protected

  - **Standards:** *How* to implement policy.
    - Source code systems are integrated with organization’s identity management system and use network password.
    - Transactions are logged to syslog and exported every 20 minutes to a log aggregation system.
Establish Goals & Team

- Initial Goals: Call to action
- Who should be involved?
- Policies & Standards
- Procedures & Assessments

RISK REDUCTION

- Achievable & Maintainable: Consistent approach to implementation
- Measureable: Evaluation if a control is in place and how it is functioning
Defining Security Criteria

• Defense-in-depth
  • Data Classification
  • Identity/Authentication
  • Access Controls
  • Isolation
  • Data Protection
  • Hardening
  • Avoiding Malicious Code
  • Logging

Forensics

Log protection
  • Restricted access
  • Storage monitors
  • Log aggregation

Regular reviews
  • One of the most common ways insiders detect breaches

Active monitoring

Restrictive access

Environment

Security

Layers of Protection

Defining Security Criteria

• Defense-in-depth
  • Data Classification
  • Identity/Authentication
  • Access Controls
  • Isolation
  • Data Protection
  • Hardening
  • Avoiding Malicious Code
  • Logging

Forensics

Log protection
  • Restricted access
  • Storage monitors
  • Log aggregation

Regular reviews
  • One of the most common ways insiders detect breaches

Active monitoring

Restrictive access

Environment

Security

Layers of Protection

Defining Security Criteria

• Defense-in-depth
  • Data Classification
  • Identity/Authentication
  • Access Controls
  • Isolation
  • Data Protection
  • Hardening
  • Avoiding Malicious Code
  • Logging

Forensics

Log protection
  • Restricted access
  • Storage monitors
  • Log aggregation

Regular reviews
  • One of the most common ways insiders detect breaches

Active monitoring

Restrictive access

Environment

Security

Layers of Protection

Defining Security Criteria

• Defense-in-depth
  • Data Classification
  • Identity/Authentication
  • Access Controls
  • Isolation
  • Data Protection
  • Hardening
  • Avoiding Malicious Code
  • Logging

Forensics

Log protection
  • Restricted access
  • Storage monitors
  • Log aggregation

Regular reviews
  • One of the most common ways insiders detect breaches

Active monitoring

Restrictive access

Environment

Security

Layers of Protection
Define Security Criteria

• We have a team
• We have basic Defense-in-Depth security solutions
• Now … draft Source Code Security Policies and Standards to document expectations
What can we do?

Understand the current environment
Where are we?

Establish a baseline

- Scope your environment
- Environment diagrams
Where are we?

Establish a baseline

- Scope your environment
  - Environment diagrams
  - Engineering practices
Establish a baseline

• Scope your environment
  • Environment diagrams
  • Engineering practices
  • Data classification: where is the important “stuff”? 
• Threat Modeling
Where are we?

Establish a baseline
- Are they working securely?
- Simple solutions?
  - Turn on functionality
  - Add-ons
- Cost/benefit
  - Change tools
  - Reinforce environment

Don't throw the baby out with the bathwater!

Scope your environment
- Environment diagrams
- Engineering practices
- Data classification: where is the important “stuff”?

Threat Modeling
- Tools
Where are we?

- Scope your environment
  - Environment diagrams
  - Engineering practices
  - Data classification: where is the important “stuff”?
- Threat Modeling
- Tools
- Usability!!!
What did EMC find?
# 2011 EMC Summary of 5 Common Brands

## Analysis of product features, not existing implementations

<table>
<thead>
<tr>
<th></th>
<th>Repository 1</th>
<th>Repository 2</th>
<th>Repository 3</th>
<th>Repository 4</th>
<th>Repository 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Out of Box</td>
<td>Add On</td>
<td>Out of Box</td>
<td>Add On</td>
<td>Out of Box</td>
</tr>
<tr>
<td>Corporate authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Logs of transactions against access controls can be exported to a monitoring tool.</td>
<td>✓</td>
<td>PARTIAL</td>
<td>✓</td>
<td>PARTIAL</td>
<td>✓</td>
</tr>
<tr>
<td>Granular access controls</td>
<td>PARTIAL</td>
<td>X</td>
<td>PARTIAL</td>
<td>X</td>
<td>PARTIAL</td>
</tr>
<tr>
<td>Support for code review workflow</td>
<td>PARTIAL</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
</tbody>
</table>
## Overall Risk Assessment Percentages

<table>
<thead>
<tr>
<th>Repository 1</th>
<th>Repository 2</th>
<th>Repository 3</th>
<th>Repository 4</th>
<th>Repository 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Box</td>
<td>Add-On</td>
<td>Out-of-Box</td>
<td>Add-On</td>
<td>Out-of-Box</td>
</tr>
<tr>
<td>TOTAL</td>
<td>TOTAL</td>
<td>TOTAL</td>
<td>TOTAL</td>
<td>TOTAL</td>
</tr>
<tr>
<td>(out of 220)</td>
<td>(out of 220)</td>
<td>(out of 220)</td>
<td>(out of 220)</td>
<td>(out of 220)</td>
</tr>
<tr>
<td>TOTAL</td>
<td>TOTAL</td>
<td>TOTAL</td>
<td>TOTAL</td>
<td>TOTAL</td>
</tr>
<tr>
<td>(out of 220)</td>
<td>(out of 220)</td>
<td>(out of 220)</td>
<td>(out of 220)</td>
<td>(out of 220)</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage</td>
<td>Percentage</td>
<td>Percentage</td>
<td>Percentage</td>
</tr>
<tr>
<td>91%</td>
<td>95%</td>
<td>73%</td>
<td>95%</td>
<td>95%</td>
</tr>
<tr>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Difference:</td>
<td>Difference:</td>
<td>Difference:</td>
<td>Difference:</td>
<td>Difference:</td>
</tr>
<tr>
<td>5%</td>
<td>23%</td>
<td>23%</td>
<td>0%</td>
<td>23%</td>
</tr>
</tbody>
</table>

### Analysis of product features, not existing implementations
EMC’s Observations

- Most major Source Code Repository systems can be made acceptable
- All existing solutions can be made better
- Newer SCMs have more security built-in or added as features
- Source code is highly visible to many people regardless of whether the SCM is distributed (like Git) or not
- A poorly configured underlying platform or poor practices can undermine strength of any application controls that may exist
Managing change …

… to steady state
Like most organizational projects ... 

- Team
- Policies & Standards
- Evaluate
- Plan
- Implement

... except this must be a continuous process.
Continuous Monitoring and Improvement

- Minimize new options
  - Until you get a handle on your environment
  - Don’t chase a moving target
- Assessments
- Security awareness training needs to emphasize secure source code
Continuous Monitoring and Improvement

- Minimize new options
  - Until you get a handle on your environment
  - Don’t chase a moving target
- Assessments
- Security awareness training needs to emphasize secure source code
- How will you evaluate new solutions?
- Expand scope: other build-related tools and infrastructure
Continuous Monitoring and Improvement

Observe & Orient

Decide

Triage

Threat Model

Assessment
eGRC
Continuous Monitoring and Improvement

- Test
- Deploy
- Implementation guidance
Summary

- Evolving threats change how we need to think about source code security
- Collaboration: Expanding security awareness involves more stakeholders
- Policies & Standards: define security goals based on common security strategies
- Measure: Baseline environment
- Implement & manage change
- Expand frameworks

**Improve security in the source code environment to defend against threats**
Thank you

Stephanie Woiciechowski, GSEC
EMC Product Security Office
stephanie.woiciechowski@emc.com