CS 493
Secure Software Systems
Incorporating SSD in SDLC

Dr. Williams
Central Connecticut State University

Objectives

- Creating an Incident Response Plan
- The Final Security Review of a system and the expected outcomes
- Periodic security reviews and archiving
- Planning system retirement and evaluating security at the end of the system lifespan
- Integrating security into the entire SDLC with both cultural awareness and available tools

Goals

- Create an Incident Response Plan.
- Identify outcomes for a Final Security Review.
- Plan periodic security reviews for a software system.
- Determine safe means of retiring a system.
- Apply the tools and practices of secure software design (SSD) to the organization's SDLC.

Incident Response Plan

One of the most essential documents to have for any system is an **Incident Response Plan**. This should include:

- what will happen if a software compromise or failure should occur
- contact personnel
- personnel availability
- procedures for multiple levels of failure

Incident Response Plan

There is no set format for an Incident Response Plan, but the following elements should be evaluated in its construction:

- Monitoring duties for the software in live operation
- A definition for incidents
- A contact for incidents
- An emergency contact for priority incidents
- A clear chain of escalation
- Procedures for shutting down the software or components of the software
- Procedures for specified exploits or attacks
- Security documentation or references for external code or hardware used in the software system

Final Security Review

The **Final Security Review** is an analysis of all of the activity that has been completed on the software prior to release.

- It is a deliverable that has an associated outcome based on whether the criteria of the system has been met
- It needs to be completed prior to the launch of the software system.

Final Security Review - Outcomes

The **Microsoft Security Development Lifecycle** includes a mandatory Final Security Review with three potential outcomes:

- **Passed:**
  - All of the metrics have been met for the system.
- **Passed with Recommendations:**
  - The system has met the security goals of the project overall, but there may be specific elements that have not matched the expectations that were set.
- **Failed:**
  - A significant metric has not been met for the project.
  - The software is not suitable for release.

Into the Wild

- Deployment is typically not an issue; the system should have been extensively tested. The problems arise when the system is in use.
- A **beta version** is a functional version of the end system in which users are expected to encounter bugs and system errors.
- When a new system is launched, it should have some form of monitoring for a specified period of time in its initial launch and ongoing monitoring that will take place after the system is fully functional and integrated.

Internal vs. External Documentation

- Creating documentation for the end user follows a security principle similar to that of error messages.
- The documentation that is released with the system should be sufficient to operate the system successfully, but it should not reveal any unnecessary details of the internal structure of the system that would make life easier for an attacker.
- This should be a consideration of balance between usability and secrecy.

Review and React

- When a modification is made to a system, it needs to undergo additional security testing.
- Any new requirements that are added to the software should go through the same iteration of security that was conducted when the system was originally developed.
- The best way to proceed is to view the additions to the system as initially untrusted elements that must pass the security screening set forth by the security level of the original system.

Evolving Attacks

- The paradigm of technology is on the side of the attacker; they get the benefit of having to succeed only a fraction of the time.
- On the security end, you have to defend all of the time and be successful all of the time.
- By mapping the security of your systems as they are developed, you have a better insight than the attacker about where the vulnerabilities of the system are found. You therefore have a better idea of where an attack will occur and what it can accomplish.

Periodic Review

Not all systems need the same level of review. To establish a reasonable timeline for review, consider the following questions:

- Is this system mission critical?
- How much privacy data is stored in this system?
- Is the system's technology still sound?
- Do the system resources still comfortably handle the usage?

Secure System Retirement

Whenever a system is removed, a description of the fate of the system components should be written into the documentation.

- **Removed:** Elements are fully retired.
- **Deactivated:** Components of the system are turned off, but are not removed.
- **Repurposed:** A component is no longer needed for an existing system, but still has value and can serve another purpose in the organization.
- **Left intact:** The component is retained; an expected lifespan should be included.

Integration Tools

The following security integration tools from the Microsoft Security Development Lifecycle are available from http://www.microsoft.com/security/sdl.

- **banned.h:** This header file should be included to deprecate the use of functions in code with known exploits.
- **Microsoft SDL Process Template:** If you are new to the integration of security into the software lifecycle, this is a very useful tool. It integrates automatically with Microsoft Visual Studio® and allows the tracking and auditing of security requirements throughout the development of the project.
- **SDL Threat Modeling Tool:** This free tool assists in the creation of threat models.
- **Attack Surface Analyzer:** This tool allows you to take a snapshot of your system before and after deployment to get a picture of added registry keys, files, locations, and resources.

Summary

- Cultural buy-in from the organization is required in order for security to be maintained and upheld.
- Important steps for a secure system on its way to release are the Incident Response Plan and the Final Security Review.
- Security does not end at deployment; the security goals established for the system are lifelong.
- Periodic security reviews are necessary to continuously uphold the security assertions of the system.
- In retirement, security should be a central focus to assert that no new holes in the overall security of the organization or its data are facilitated by the removal of the system from operation.

In class exercises revisited

For our case study: Pose questions and vote system

Assume company on the order of 200 employees

Create an incidence response plan

- Monitoring duties for the software in live operation
- A definition for incidents
- A contact for incidents
- An emergency contact for priority incidents
- A clear chain of escalation
- Procedures for shutting down the software or components of the software
- Procedures for specified exploits or attacks

Bob's Pizza Shack

In groups consider this scenario

Bob is a small business owner of Bob's Pizza Shack and wants to create a website to allow online credit card delivery orders

Create an incidence response plan

© Chad Williams Oct-17
Adapted slides with permission from Jones & Bartlett Learning, copyright 2013

Alice's Online Bank

In groups consider this scenario

- Alice opens Alice's Online Bank (AOB)
  - Internal use bank employees
  - Interoperates with another bank
  - Interacts with customers
    - Web
    - Mobile app

Create an incidence response plan

(Assume 1000s of employees)

© Chad Williams Oct-17
Adapted slides with permission from Jones & Bartlett Learning, copyright 2013

Location based social media app

In groups consider this scenario Open source group wants to create a mobile app to allow groups to communicate/find each other in public demonstrations/protests

- Communication internet, as well as, P2P (WiFi/Bluetooth) in case internet cut off – so if person you want to contact is on other side of crowd and no internet as long as P2P network can be established with app can reach somebody outside your immediate vicinity via the P2P network
- Should be able to communicate securely messages and images to people you identify within your group (group as whole or direct)
- Should be able to share GPS location with people in group (group as whole or direct)

- Incidence response plan?

© Chad Williams Oct-17
Adapted slides with permission from Jones & Bartlett Learning, copyright 2013