



Interested in learning  
more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Pre-Development Security Planning

Security should be considered from the onset of any development project. There are several crucial steps that project developers and project managers can take before code development begins that can significantly improve the entire development cycle and avoid potential security pitfalls that would otherwise arise. This document will outline the basic steps that should be completed before code development begins to ensure delivery of a successful project.

Copyright SANS Institute  
Author Retains Full Rights

AD

Veriato

Unmatched visibility into the computer  
activity of employees and contractors



Try Now

## **Pre-Development Security Planning**

Keith Marohn

August 13, 2001

### **Introduction**

Security should be considered from the onset of any development project. There are several crucial steps that project developers and project managers can take before code development begins that can significantly improve the entire development cycle and avoid potential security pitfalls that would otherwise arise. This document will outline the basic steps that should be completed before code development begins to ensure delivery of a successful project.

### **Determining Ownership and Responsibility**

One of the most important aspects of managing a secure and successful project is to identify the responsibilities of each group involved with development and streamline communications by identifying a single authoritative contact from each group. To enforce accountability the authoritative contact from each group should sign a written agreement stating their role and responsibilities. The various groups that ought be represented during pre-development will vary with each project. However, there are a few key groups necessary for successful delivery of any project.

Development should never begin without first identifying the project owner. Project owners are responsible for making final decisions about a project. In situations where the projects owner is actually a group, a single authoritative contact should be identified to represent the group during project development. In some situations ownership may be very clear and evident and in other cases identifying the owner may be more obscure. Here are some questions to ask that will help you identify the project owner:

- Who requested the project?
- Who owns the data utilized by the project?
- What function will this project serve?
- Who will maintain this project after development is complete?

Project developers are responsible for coordinating project development and delivering a project that will perform to the specifications defined by the project owner. Project developers should be able to identify the vulnerabilities of a project and recommend security measures that can be used to eliminate or reduce those vulnerabilities. Project vulnerabilities that prohibit compliance with project specifications are the responsibility of the project developer. A single authoritative contact should be identified to represent the project development group in situations where there are multiple developers. If multiple development groups exist, a single authoritative contact should be identified to represent each development group.

In addition to the project owner and project developer it is good practice to identify the other groups impacted by a project. Representation by all groups is typically beneficial and is often absolutely necessary to the success of a project. Network Administrator's are bound to have legitimate concerns over bandwidth issues and firewall rules of any new project. Likewise, System Administrator's will need to identify hardware requirements for supporting servers and Backup Operators will need to make plans as well. At a minimum these groups should be in communication with the project developer.

### **Identify The Project Purpose and Requirements**

Project identification is the key to understanding a project's vulnerabilities. A written description of the project including a statement detailing the purpose of the project and any requirements placed on the project by the project owner should be prepared and signed by the project owner and project developer before beginning code development. Project descriptions may range from a brief paragraph to several pages in length. Diagrams, flow charts, and other documentation may be included as necessary. This description does not need to include every project detail, but should be defined well enough so that someone unfamiliar with the project could understand the project's purpose and requirements.

### **Identify the Data and Permission Requirements**

Describe each group of data that will be accessed, managed, manipulated, or transferred by the project. Define the systems or user groups that will have permission to access and manipulate each group of data. Describe who has authority to assign and revoke permissions for each data group. Identify the current and potential quantities of data that will be involved and identify the acceptable parameters of all data. This type of information may seem like unnecessary details in early planning stages and is easy to overlook. However, understanding the data is the key to understanding how to secure the data and is essential for avoiding problems later in development. Here are a few specific items that should be defined prior to beginning code development

- Identify acceptable formats and ranges for date fields
- Identify the precision and acceptable ranges of each numeric field
- Identify the minimum and maximum lengths of each string
- Identify any character limitations of strings such as Unicode character support or A-Z type limitations
- Identify acceptable units (*e.g.* Will currency be tracked in US Dollars or Eurocurrency)
- Identify the quantity of data that the project should be designed to handle.
- Identify the quantity of data that the project should be designed to process during a given time period.
- Identify the maximum number of users that will have access to read or modify a particular group of data at any one time.

## **Identify the Users**

Identifying the user groups will often provide insight into how the project will be used. Identify how many users will be on the system; identify that the established data parameters will accommodate the user groups; and identify the physical environment of the users. If users will be accessing the project from remote connections across the Internet security measures will likely be different than if users were all located within a single secure building.

## **Identify Supporting Systems and their Vulnerabilities**

Describe each system that will be utilized by the project. System descriptions should identify the group responsible for managing the system as well as the minimum hardware requirements of the system; operating system; particular service pack when relevant; any software dependencies of the project; and any other system requirements. If the project is being designed for cross-compatibility describe each system that the developer will need to support. Define any relevant details about the security measures that will be used for each system as well as the system's vulnerabilities. For example you may define that the system has a backup power reserve of four hours. This would alert project managers that additional hardware will need to be purchased if downtime from long-term power failures is not acceptable.

When determining ownership of systems describe the owner as the largest relevant group. For example if the system is owned by another business describe the owner as that business entity, not the current employee who will be administering the system. This correctly places the responsibility on the management group and prevents questions in the event that an employee leaves the company or restructuring eliminates a particular position.

In cases such as the Internet where describing each of the systems or components involved in transferring the data would not provide beneficial details it is alright to simply group the systems as a whole.

The technologies and coding languages that will be used should also be determined before beginning code development. Use of technologies with known security issues should be avoided. Additionally, each technology should be reviewed for compatibility issues with the other technologies being utilized. Technologies need to match the program requirements. For example an Access Database would never be used to store sensitive customer information.

## **Identify the Threats**

Identifying the threats that your project may face will help in identifying the vulnerabilities and will assist in selecting the appropriate security measures for protection. Threats may be environmental such as flood, fire, or power failures; users may also threaten the project with carelessness, mischief, ignorance, or theft; systems may threaten the project with potential hardware failures or poor performance; non-authorized use and non-intended exploits of the projects designed functionality may also threaten the project.

## **Identifying Vulnerabilities**

Project owners cannot make sound decisions for the project unless the vulnerabilities have been identified. It is important that the project owner understand that Trojan programs running on clients, long-term power failures, and network outages are potential vulnerabilities. The project owner must then decide whether backup generators, redundant network links, and tighter security controls need to be implemented for the project. These decisions will greatly affect project development and need to be identified before coding begins.

Identify how vulnerable a system is to scaling difficulties. Project developers should be able to provide an estimate as to the maximum abilities of the project and should identify how well the project will scale if needed. Additionally, a project should be reviewed from a manageability standpoint. Projects that are difficult to manage when implemented will be more susceptible to security problems..

## **Identify the Security Measures to be Used**

From the project description you should have a clear understanding of the project, including the flow of data, data parameters, permission requirements, and the relationship of the supporting systems. From this information you will be able to identify what data needs protection, and the vulnerabilities that exist. By carefully selecting the security measures to be used you will eliminate or reduce vulnerabilities to a tolerable level.

## **Authentication**

Authentication is used to validate the source of data and should be used whenever data is transferred between systems or terminals. The method of authentication will vary greatly depending on the exact implementation and may range from use of anonymous guest accounts to multiple authentication methods used in parallel. The authentication method or methods chosen for a project should reflect the project's security requirements.

## **Security in Transport**

While authentication is used to identify the source of the data, transport security is used to ensure data confidentiality and integrity as the data stream is transferred between systems. Forms of transport security may include network segmentation, utilizing private communication lines, encrypting data, and physical security. As with authentication, the methods employed for transport security should reflect the security requirements of the project.

## **Physical Security**

The security of any system is only as good as its physical security. Project development may not be dependant on physical security of the supporting systems, but project owners would be remiss to not consider physical security as a project vulnerability. Project owners should require a written agreement with system owner's that defines the security expectations and requirements of each system. Physical security not only includes restrictions on access to the system, but also includes protection from fire, floods, wind, and power outages.

## **Data Parameters**

Data validation is essential to security. Data parameters should be defined as well as the locations within the data flow that validation will occur. When possible at least rudimentary data validation should be handled on the client before the data is transferred to a server. However, client side validation should never be used to replace server-side validation.

## **Signing-Off on the Project for Development**

Whether a project will be managing sensitive data or a web page is being developed to provide information free to the public, it is essential that a written statement describing the project's security measures and vulnerabilities be signed. By signing-off on a statement describing the project's security, each group will take responsibility for the decisions they have made. Additionally, communicating the project requirements to the different groups involved may aide in identifying potential security problems that may not have been noticed until latter in development.

After all necessary information has been put together it should be distributed to the project owner, project developer, and the owners of the supporting systems for review. The owners should then distribute copies of this report to their direct contacts as necessary. There are bound to be questions and revisions as copies of the document are distributed to System Administrator's, Network Administrator's, Information Security Officer's and the various people that will be working directly with the project. Make sure you allow plenty of time for the document to be reviewed and revised. It is essential that questions and concerns be worked out prior to beginning code development.

It is important that each group be comfortable with signing the document and that no group signs-off for requirements which they cannot support. If the Network Administrator has concerns about bandwidth or Server Administrator's have concerns over load then the requirements should be further defined before the agreements are signed.

## Conclusion

By utilizing the suggestions in this document you will be able to identify the project's security needs and provide the best solutions to reduce or eliminate the vulnerabilities that a project will face. After development is complete you will be able to review the project to verify that the agreed upon security requirements have been met.

## References:

Information Technology Security Practices  
<http://csrc.nist.gov/bestpractice/>

The World Wide Web Security FAQ  
<http://www.w3.org/Security/Faq/>

Security for Information Technology Service Contracts  
<http://www.cert.org/security-improvement/modules/m03.html>

Planning Distributed Security  
[http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Deploy/dgbe\\_sec\\_zyua.htm](http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Deploy/dgbe_sec_zyua.htm)

Keys, Internet Management, CRC Press LLC, 2000 ISBN 0-8493-9987-4

© SANS Institute 2002, Author retains full rights.



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Amsterdam May 2018	OnlineNL	May 28, 2018 - Jun 02, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced