Secure Coding.
Practical steps to defend your web apps.

Defining and Understanding Security in the Software Development Life Cycle

James E. Purcell

Defining and Understanding Security in the Software Development Life Cycle

Introduction

The purpose of this paper is to help you understand the important role that security plays in the Software Development Life Cycle (SDLC). The paper defines security as it applies to the SDLC and discusses overall SDLC security issues. It then covers each phase of the SDLC and specific security controls and issues for each phase. After discussing the SDLC, we apply its uses to a fictitious company to illustrate the concepts.

Note that the SDLC acronym is also used to represent System Development Life Cycle. In many cases, a decision is made to purchase or outsource the software and associated hardware and network systems needed to implement a new application. This is often referred to as the "buy or build" decision. Buy means you will purchase a finished product from a vendor and build means you will hire someone to develop it for you. This paper focuses on the Software Development Life Cycle, but most of the phases, terms, and issues discussed apply to both the "buy" and "build" process.

Definition of Security in the SDLC

When defining security in the SDLC, two areas must be addressed. The first area is the SDLC process itself. The second area is application operational security. You must understand the SDLC process and associated security activities *and* the specific application and operational security controls that are available to the application designer.

Security in the SDLC Process

The SDLC process consists of six phases (discussed in detail later). In each phase, specific security related activities take place to ensure that security is built into the software system under development. For example, in one phase, SDLC Project Initiation Phase, a security related activity is to define the sensitivity of the information that the software system will process. By placing this security related activity early in the SDLC process, later decisions are made based on the security needs of the organization and not as an afterthought.

Application Operational Security

As the development team moves through the phases of the SDLC, decisions are made to add security controls to the application to ensure the proper protections to confidentiality, integrity, and availability. These application and operational controls can be administrative controls, physical controls, or technical controls. An example of an administrative control designed into the application in the Operations and Maintenance Phase is Separation of Duties. In each SDLC phase, example applications controls that are appropriate for the phase are defined and discussed.

SDLC Security Issues

The goal of a good SDLC process is to capture, verify, and implement all the requirements needed to make the application useful to the organization. These requirements include security needs defined around confidentiality, integrity, and availability of the information system. If security requirements are correctly identified and the proper security controls added are to the application to meet these requirements, the result is a secure application. But in reality, developing applications involves trade-offs to meet budget, resource, and time constraints placed on the project. In many cases, security is the first requirement to be dropped.

Another security SDLC issue is the lack of security training and knowledge among developers and system designers. Poor design decisions are made when developers are not aware of current security risks. As a result of these SDLC security short comings, security is often an afterthought, and security controls are implemented as add-ons after the project is complete and security issues come to light. Applications built this way become overly complex, expensive, and hard to maintain. This ensures that security is further compromised and the application system suffers from continued security problems.

Even if a system is designed and developed with security in mind, systems change over time. New equipment, software, and functionality are added to systems regularly over time. These changes must be authorized and tracked, and security issues need to be evaluated as part of a configuration management process.

The rest of the paper describes how to build in security at each phase of the SDLC and discusses typical controls at the disposal of the system designer to guard the confidentiality, integrity, and availability of the application. The example application described is a customer information system for GIAC Bikes. GIAC Bikes is a company that designs and sells custom trail bikes at both its retail store and over the GIACBikes.com website.

SDLC Phases

Project Initiation

In the Project Initiation Phase of the SDLC, GIAC Bikes determines the need for the customer information system. The business needs the system to allow GIAC Bikes to better track customer buying habits and preferences to better plan future bike designs and marketing plans. If no business case for the system can be made, this is the time to drop the system project before any more time or money is spent.

The security activity that the GIAC Bikes system development team performs in this phase is a preliminary risk assessment. The design team looks at several risk areas, including sensitivity of information collected, criticality of the system to GIAC Bikes, security risks in common to customer information systems, and regulatory, legal, and privacy issues pertinent to customer information systems. The system design team assigns high, medium, and low risk values to each area of risk. For instance, because

GIAC Bikes does business in Europe (where privacy laws are strong) and the customer information system collects personal data, risk and impact of the confidentiality of the system information is high. In another example, although the customer information system is important to GIAC Bikes, business can continue if the system became unavailable for a long period of time. Therefore, the design team assigns a low risk value for system availability. Doing the preliminary risk assessment to establish the need for the system helps identity any security show stoppers before too much time and effort goes into the next SDLC phases. It also gets the design team thinking about security issues early in the design process.

Design Analysis (Functional Design)

The Design Analysis Phase is where the design team thinks about and documents specific functions that the system should carry out. For the GIAC Bikes customer information system, some system functions include collecting customer information (input), verifying data integrity (processing), and reporting customer preferences (output). An additional functionality of the system is to backup and restore the customer database.

There are two security activities that take place in this phase. The first security activity is to perform a more detailed risk assessment for each major system function and for the overall system. Based on this detailed risk assessment, security controls are selected to mitigate the risks identified. For example, because there is a high risk that backup media can be lost or stolen, the design team specifies that encryption is applied to the backup media to mitigate this risk. Encryption is an example of a control that can reduce risk. For a comprehensive list of administrative, technical, and physical controls that can be applied to an information system, see the NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems”. Now the design team has the functional requirements for the GIAC Bikes customer information system and for each functional requirement a level of associated risk and possible security controls to reduce (or mitigate) that risk.

System Design Specifications

In the System Design Specification phase, the Functional Design from the Design Analysis Phase is translated into detailed specifications. For instance, the functional need for storing customer information for the GIAC Bikes customer information system is turned into a database schema. The functional need to have customer reports is translated into report layouts.

The security activities associated with phase are to design the actual security controls specified in the Functional Design. For instance, the actual method and algorithm for encrypting the backup media is specified. Another security activity in this phase is to review the completed design specification for any new security issues that have surfaced during detail design. An example here is that the GIAC design team chooses Oracle as the DBMS system for the customer information system and new security controls are specified because of known weaknesses in Oracle database security. At this point in the SDLC, the GIAC Bikes customer information system design team has designed security into the system based on a risk assessment of threats against the confidentiality, integrity,

and availability needs of GIAC Bikes.

The System Design phase is the SDLC phase where most application security controls are specified. Application controls are applied across input processes, information processing processes, and output processes. Examples for the GIAC Bikes customer information system include:

- Input—Testing all input values for correct syntax and data ranges
- Processing—Transactions are logged and checked for referential integrity
- Output—Access to data output screens and reports are allowed only to authorized uses with an access control system

Programming and Testing

With the design specifications in hand, the focus of the SDLC moves to the programmers. Programmers take the detailed design specifications and begin to translate them into program code.

Security activities that take place in this phase include auditing the programs code to ensure that secure programming practices are implemented. In addition, programmers must test the code to ensure security controls work as designed. Note that although programmers perform unit testing on their own code, separation of duties dictates that the system test be performed by a group other than the programmers. System testing is usually the job of the QA function. GIAC Bikes programmers code and test individual system modules (input screens, database processing, report programs) and the GIAC Bikes QA team performs a system test of all the modules. However, both the programmers in the unit and QA in the system test one major area: They both perform tests to make sure that all system input is validated. For example, if a user attempts to inject raw SQL commands into an input field to return all customer information, the system should detect and block the attempt.

The goal of unit and system testing is to certify the system meets the design requirements set forth in the earlier SDLC phases. Security functions are tested to ensure they provide the needed level of protection. For GIAC Bikes, the encryption method for the backup media is tested to make sure the encryption is not easily defeated and that the backup data can be restored according to the documented procedure. Any security shortcomings are also documented in the certification process.

Installation and Maintenance

In the Installation and Maintenance phase the system is fielded and enters the operation and maintenance (O&M) stage.

However, before the system is made, operational management signs off on (or accredits) the system. Management makes the accreditation decision based on the certification report from the Programming and Testing phase. For GIAC Bikes, management looks at the testing results of all the security controls and decides that the risks of running the system have been properly addressed. Based on that decision, the system goes into

production mode.

Because no system stays the same for long, an important security element in this phase is configuration and change management. As changes to the system are proposed and implemented, the changes must be carefully analyzed for security impacts. For example, the GIAC Bikes customer information system is so successful that GIAC Bikes business doubles within a year. To handle the increased database processing needs, it is proposed to upgrade to a newer version of the database software and increase the capacity of the database server hardware. As a part if its change control process, GIAC Bikes customer information system development team analyzes any issues that affect the confidentiality, integrity, or availability of the system during the upgrade.

The Installation and Maintenance Phase is another SDLC phase where application and operational controls are important. Two example application operational controls important to GIAC Bikes are accountability controls and separation of duties controls. To implement accountability of the GIAC Bikes customer information system, an access control systems is used to authorize and log all user accesses and changes to the database. These logs are examined regularly and any attempted unauthorized activity is investigated. Separation of duties is also implemented with an access control system that allows levels of system access based on the need of the user to know the customer information. For instance, a data entry clerk can enter basic customer information, although the clerk cannot see the customer order history. A product pricing analyst can see aggregated pricing information; however, the analyst cannot see individual customer records.

Destruction

In the Destruction phase of the SDLC, the system is retired and replaced with a new system.

The main security activity in this phase is to ensure that any sensitive information is properly handled. The data might need to be securely archived or completely destroyed. The Destruction phase can also be invoked during system upgrades. When GIAC Bikes upgrades the database server, the development team makes sure that the disk drives on the old server are properly scrubbed of any sensitive GIAC Bikes customer information before the old server is repurposed or disposed.

Summary

If companies follow the SDLC phases and incorporate the appropriate security activities in each phase, systems can be developed in a secure manner. If security is not built in to the system in this manner, the security shortcomings of the system will be discovered. IT auditors might find the problems and dictate that costly system changes be implemented. Or, attackers might find the problems and cause damage to company assets and reputation. GIAC Bikes has followed the SDLC phases and has considered security issues at every step. This has allowed GIAC Bikes to develop, deploy, and maintain a successful and secure system.

Last Updated: June 26th, 2017

Upcoming SANS App Sec Training

SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Minneapolis DEV534	Minneapolis, MN	Aug 25, 2017 - Aug 28, 2017	Community SANS
Community SANS San Francisco DEV541	San Francisco, CA	Aug 28, 2017 - Aug 31, 2017	Community SANS
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Secure DevOps Summit & Training	Denver, CO	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - DEV522: Defending Web Applications Security Essentials	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced