American Journal of Mining Engineering.
1(1):20-22, August 2019

Research Paper

AppSec Chain, Secure SDLC with Block chain.

Shoba Jagathpal

Information Security Professional, Bengaluru, Karnataka, India.

To cite this article: Shobha Jagathpal. AppSec Chain, Secure SDLC with Block chain. American Journal of Materials Engineering,1(1):20-22,May-June 2019.

Email: shobhajagathpal@gmail.com

Received: 27th April 2019.| Revised: 24th May 2019.| Accepted: 21st June 2019.

Abstract: Application security involves providing measures to ensure security of all applications in an enterprise. Safe guarding application is aimed at detecting and preventing exploitation of known or unknown vulnerabilities by any of internal or external threats from applications. It's very common that applications in an enterprise can be either be developed completely in house or bought from vendors. This paper provides block chain based conceptual approach to track and verify secure software development life cycle for applications developed in-house as part of enterprise security initiative related application security area.

Keywords: Application Security, Software Development Life Cycle (*SDLC)*, Block chain.

1. Introduction

Cyber security has gained greater importance from last few years as the number of vulnerabilities being discovered in applications causing business impact is far greater than the number of vulnerabilities discovered in operating systems. Due to the current trend of attacking every digital asset offered by any enterprise - be it a website, mobile application or *IoT* device, it becomes at most importance to track and verify each of the application security measures implemented in enterprise as part of application security initiatives and take quick remediation steps in areas where deviations are found.

2. Software Development Life Cycle

Foundational measures taken by any enterprise as part of application security measures to safe guard threats from applications built internally is by means of implementing threat modelling, static and dynamic code scanning, penetration testing, driving remediation's of critical exploitable vulnerabilities, secure code reviews and training developers on best practices for coding.

While the business and security teams figure out ways to collaborate and ensure security controls are imbibed all through software development life cycle, this paper talks about an approach for implementing application security measures for secure software development life cycle with mechanisms to perform integrity check, controls verification and tracking application development phase. The approach shared is at conceptual level. Feasibility and probable challenges that can come during implementation will be experimented and shared.

Software Development Life Cycle *(SDLC*) for any enterprise typically has 4 to 8 phases depending on how enterprises adopt it. There could be explicitly calling each phase or combining scope of one or more phases in single phase to have enterprise *SDLC* phases.From *NIST* **[1],** *SDLC* comprises of the 5 phases as below. For each phase, an in-house application development would involve scope as below.

- Initiation – relates to requirements gathering
- Development/Acquisition - relates to design and development
- Implementation/Assessment – relates to deployment of the solution developed in-house
- Operation/Maintenance – relates to support, enhancements of the solution and maintenance
- Disposal – relates to decommissioning of the solution

NIST clearly guides on security controls that should be taken care at each phase in *SDLC*. There are other standards and guidelines available for secure SDLC from *SANS* **[2],** *OWASP* and others. Most well-known among them is from OWASP. For the approach I share below, *NIST* publication will be used as reference to refer to secure SDLC phases.

3. Block chain for Secure SDLC

Block chain put in very simple words is a chain of blocks helping to exchange information between peers called as transactions in a distributed way. Details of the block and entire chain is available publicly and by nature it provides integrity of the contents in the chain.

Now, how do we apply the concept of Block chain to application security needs?

As of now Block chain is widely used as cryptocurrency. They are used on transactions to buy/sell/hold/gain/gift/transfer any asset. Smart contract is a concept which enables applying block chain concept in other areas. We will be leveraging the concept of smart contract to meet application security area needs to track and verify application security measures.

4. Mapping of *SDLC* phases to Block chain transactions

Assuming the enterprise has deployed foundational process and tools assisting in implementing application security measures, it's easy to map *SDLC* phases to application security measures. Once an attempt to map each *SDLC* phase of *NIST* to an application security measure is done, it becomes obvious that each of the secure *SDLC* phases from *NIST* having a corresponding application security measure should be tracked and verified to ensure enterprises have controls for stage gate implementation and identify deviations of application security measures on applications that gets deployed in production, maintained or decommissioned in enterprise.

Do we really need to use block chain here? Why can't the traditional approach of centralized management of services work?

Of course, traditional approach of having a centralized monitoring of services will be a perfect fit for tracking and verifying each of the secure SDLC phases. As the size grows, volume of applications increase, centralized service should be scalable to support and meet performance needs for every tracking and verification flow. This would also need network resource utilization. Block chain based approach is an alternate of centralized management and using block chain the inherent benefits of de-centralized, integrity verified solution can be leveraged. It can help track and verify every application go through the application security program measures.

How to start?

Let's start with first phase of secure *SDLC* and identify if there are opportunities to infer attributes that should be considered as transactions in block chain. This will help us validate completion of a security measure adherence and help verify deviations to remediate. A block is nothing but a record with details on transactions in a block chain. As a block, it can literally contain any kind of information to help us track application security measure. We'll compose secure SDLC block chain called AppSec Chain to have blocks with following details using bitcoin as a reference implementation

- Version (4 bytes)
- Hash of the previous block, thus making a chain of block (32 bytes)
- Merkle root, the tree of transactions' reference (32 bytes)
- Timestamp, number of seconds since 1970-01-01 00:00 (4 bytes)
- Bits, a representation of the networks current difficulty (4 bytes)
- Nonce, incremented when mining (4 bytes)

A chain of AppSec chain blocks with above details now should help us track and verify each phase SDLC the application flow has gone through and their adherence to application security measure. In order to use this approach, AppSec team is required to know all the applications of enterprise. AppSec team hence is well placed to provide ways to integrate with enterprise identity service and provide identity for applications. During the first phase of secure SDLC they provide a unique global id for application, AppUid. This will be the first transaction going into block. Similarly, possible transaction details that can go into block are shown in figure 1.

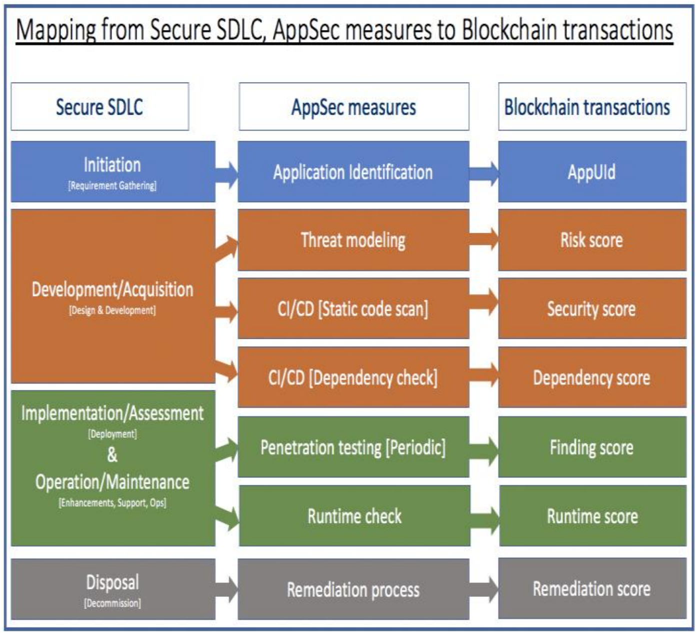

Figure - 1: Mapping of secure SDLC from NIST to AppSec measures and corresponding Block chain transactions

How to arrive at appropriate score value to measure each application security measure?

The recommendation is to have score of each application security measure to be assigned a value from 1 to 100. Any of existing frameworks or guidelines can be used to arrive at the same. For Eg, OWASP risk scoring methodology can be used to arrive at penetration testing score. The final score should be of 1 to 100 in range. A block in AppSec chain for us now will now have the following info in transactions

- AppUid
- Risk score
- Security score
- Dependency score
- Finding score
- Runtime score
- Remediation score

Block chain of the application can be visualized as below

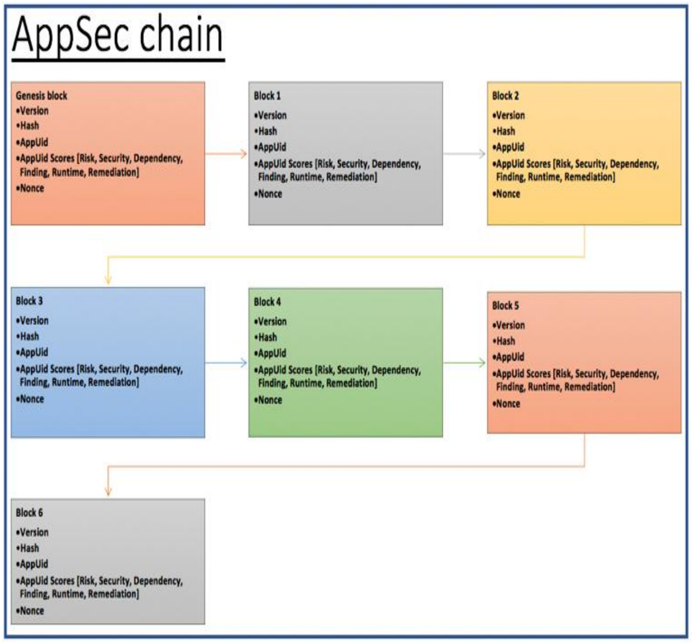
AppSec chain
Genesis block
•Version
•Hash
•AppUid
•AppUid Scores [Risk, Security, Dependency, Finding, Runtime, Remediation]
•Nonce
Block 1
•Version
•Hash
•AppUid
•AppUid Scores [Risk, Security, Dependency, Finding, Runtime, Remediation]
•Nonce
Block 2
•Version
•Hash
•AppUid
•AppUid Scores [Risk, Security, Dependency, Finding, Runtime, Remediation]
•Nonce
Block 3
•Version
•Hash
•AppUid
•AppUid Scores [Risk, Security, Dependency, Finding, Runtime, Remediation]
•Nonce
Block 4
•Version
•Hash
•AppUid
•AppUid Scores [Risk, Security, Dependency, Finding, Runtime, Remediation]
•Nonce
Block 5
•Version
•Hash
•AppUid
•AppUid Scores [Risk, Security, Dependency, Finding, Runtime, Remediation]
•Nonce
Block 6
•Version
•Hash
•AppUid
•AppUid Scores [Risk, Security, Dependency, Finding, Runtime, Remediation]
•Nonce

Figure - 2: Blocks of AppSec Chain for an application

As the application passes through various phase in secure SDLC, the AppSec team validates, signs and add block to the chain. This should be stored by application. AppSec team will validate at any point of time the deviations an application goes through in entire life cycle. To build a solution based on this concept, AppSec team should offer services which can act as AppSec Identity Provider, AppSec Validators which act as Miners in the enterprise.

An additional step that can be taken during the entire secure SDLC flow is to maintain 2 lists to have hashes of all applications. While generating AppUid, AppSec Identity Provider will compute a hash h of the public key of the application, it stores the key-value pair (h, 1) in a block chain that it controls to have all application. If an application is decommissioned, the AppSec team places the same in another block chain store it controls. This will enable the enterprise at any point of time to be aware of all applications that are running securely and the once which are decommissioned. Though this information is very much available as part of AppSec chain for each application, may not fit into the block chain decentralized concept, maintaining it as an additional step by AppSec team will help simplify adoption of the proposed concept. Established for the inputs to produce the expected output.

5. Conclusion

Software The use of block chain is scoped to assist enterprise track and verify application’s adherence to secure SDLC phases with respect to application security measures. Working through implementation will solidify the feasibility and challenges of the approach.

References

1. NIST Special Publication (SP) 800-64, Revision 2, Security Considerations in the System Development Life Cycle.
2. https://software-security.sans.org/resources/paper/cissp/building-security-system-development-life-cycle-sdlc-case-study.

Bibliography

Shobha Jagathpal is an information security professional experienced in enterprise application development and consultation. She has managed all aspects of Software Development Life Cycle in security domain delivering world class products.