HYPERLEDGER GLOBAL FORUM

June 8–10, 2021 | Virtual Experience

#hyperledgerforum

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

银行业区块链基础设施安全审计的思考

Terry 万勇 , Hyperledger TWG 中国工作组志愿者

日益增加的安全性挑战

安全性的挑战

- 容器的安全现状。
- 基于容器的区块链基础设施的安全现状。

容器的安全现状

- Container 容器技术日益成为现代软件开发的首选。 Gartner 的数据，到 2023 年，超过 70% 的组织将采用容器技术。
- 但在安全方面，根据一项 2020 年全球 调查发现， 56% 的开发人员根本不运行容器扫描，而且大多数团队没有针对容器或许多其他尖端软件技术（包括云原生 / 无服务器、 API 和微服务）的安全计划。

区块链基础设施的安全现状

- 区块链基础设施大多数运行在容器中，这导致容器的安全问题威胁到基于容器的区块链基础设施的安全。
- 很多 Fabric 项目采用 K8s 作为部署和管理的平台，这使得 K8s 的安全性变得重要。
- 在本文中，我们将探讨可能遇到的一些安全风险和挑战，以帮助您确保区块链基础设施和应用的安全。

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

Hyperledger Fabric 的安全策略

容器架构改变了安全策略和要求

- 容器架构具有更多的抽象层。

  虚拟机只有主机操作系统、虚拟机操作系统、虚拟机 APP 运行环境。传统物理机的软件层更少，安全情况更简单。在生产容器环境中，需要专门的工具来监控和保护这些抽象层。例如：主机操作系统、容器运行时、编排器、容器镜像私有 Registry 、网络层。

- 容器封装了所有的依赖关系，安全性嵌入了 APP 全生命周期

  手动创建和维护每个实体的安全规则是不切实际的，将安全检查集成到 CI/CD 工作流程，并实施 DevSecOps

Hyperledger Fabric 的安全策略

按照维度，引入容器的安全策略：

- 容器架构抽象层的维度。
- 应用 APP 生命周期的维度。

容器架构抽象层的维度

- 镜像、镜像 Registry
- 生产级别的容器编排系统 (K8s)
- 容器、容器运行时（ Docker, runC, cri-o, containerd ）
- 主机

镜像漏洞和合规性

- 镜像进行漏洞和合规性扫描。

  建立适当的扫描规则，检查配置文件里暴露的明文密码、恶意软件等。使用最小的基图，构建镜像层，不添加不必要的组件。把镜像扫描集成到 CI/CD 管道。

- 关注镜像的时效性。

  随着时间推移，可能会发现，之前被认为安全的组件中的漏洞，需要给镜像设置时间阈值。

镜像 Registry

- 确保从可信的镜像 Registry 获取镜像是一项核心的安全要求。
- 对托管镜像 Registry 的服务器进行漏洞和合规性扫描。
- 锁定上述服务器，使用安全访问策略。例如，设置白名单，只允许访问特定的镜像 Registry 。

生产级别的容器编排系统 (K8s)

- 安全和基础设施团队需要制定适当的访问控制措施，以防止来自过度使用特权帐户、网络攻击和不必要的 pod 到 pod 之间的横向移动的风险。
- 确保用户只使用适当的角色执行命令，减少使用特权用户。
- K8s 提供丰富的配置选项，但默认值通常最不安全，例如：默认情况，不会限制 pod 到 pod 的通信，攻击者可能利用 pod 横向移动，实施攻击。

生产级别的容器编排系统 (K8s) - 续

- 凭据和密钥等敏感数据必须选择存储和访问方式。例如：必须确保凭据和密钥不会作为环境变量传递。
- 尽可能更新到最新版本，及时安装补丁程序。禁用匿名访问 kubelet，启用 TLS 等。

容器、容器运行时

- 容器运行时是容器技术栈中较难保护的部分之一。传统的安全工具不适用于监控运行中的容器的。它们无法深入容器内部，也不适用于建立容器运行时的安全基线。
- 及时更新容器运行时到最新安全版本，为其容器环境建立行为基线，以防止异常或攻击。
- 引入“不变性”概念， APP 应用或服务更新时，用新的容器替换现有容器。“不变性”具有安全优势，用户无法在容器上更改配置管理和安全策略。

主机

容器环境的主机操作系统是容器技术栈中最重要的一层，涉及主机环境的攻击行为可能导致入侵者有权访问整个容器运行环境的任何内容。这就是为什么主机需要：

- 扫描漏洞。
- 设置安全加固基线。
- 更严格的访问控制（禁止 Docker 命令、 SSH 命令、或文件篡改等）。

应用 APP 生命周期的维度

- 遵从 " 前移 " 原则，镜像构建的阶段就开始引入安全措施，避免后期花费更多成本。
- Build 阶段：这里主要指，构建并扫描镜像，避免已知的漏洞。
- Deploy 阶段：在部署方案中，引入安全措施，隔离重要的工作负载；检查镜像有效期；合理设置 pod 的特权级别；使用密钥管理工具；禁用 K8s 默认的配置选项，防止攻击者闯入时，跨容器的横向移动。

应用 APP 生命周期的维度 - 续

- Runtime 阶段：监控各项指标，尽早发现异常行为。例如：系统资源占用率、 Network-level 的流量，交易完成率。
- K8s 和容器运行时的主机 (全周期)： 对这些基础设施，采用抽象层所述的安全策略。

Build 阶段

- Fabric 的镜像都是官方给出的，不用自行编译，主要确认从可信的镜像 Registry 下载镜像。减轻了安全顾虑。
- 指定镜像 Registry ，仅使用“白名单”中的已知镜像 Registry 。
- (如有) 对托管私有镜像 Registry 的服务器进行漏洞和合规性扫描。

Deploy 阶段

- CA 证书产生的密钥代表了区块链交易参与者的唯一身份，是需要关注的重点。
- 使用密钥工具管理 CA 证书和密码，例如： Hashicorp Vault ； 也可以选择硬件安全模块 （ HSM ） 或加密持久卷 （ PV ） 。
- 把每个组织隔离在不同的 namespace 中，例如： order 和 peer 就分配在不同的 namespace 。
- 设置合理的 NetworkPolicy ， 禁用 K8s 默认配置，防止攻击者利用 pod 的“横向移动”实施破坏。 该项需对整体架构有一定理解，采用多种规则组合，较复杂，本文只提概念。

Runtime 阶段

- 监控各项指标，尽早发现异常。对于具体的监控指标，试运行一段时间，随需增减，没有统一的要求。原则是监控区块链基础设施平稳运行。
- peer 、 order 节点所使用的资源。例如：随着加入到更多的 channel ，其 CPU 和内存的增长率应该呈现合理的线性增长。
- 存储占用率，保证足够的空间分配给 State DB 和区块。
- 网络安全事件日志告警（例如，被阻塞或接收的连接请求）

内部审计与三道防线

前言

- 本文旨在叙述，作者以 IT 技术专家的身份，“借调”到审计团队，从事银行信息系统 IT 审计的一段经历。从技术人员的角度，阐述 IT 审计过程需要思考的问题。不足之处，请见谅。
- 文章涉及的内容已移除敏感信息。

商业银行的“三道防线”

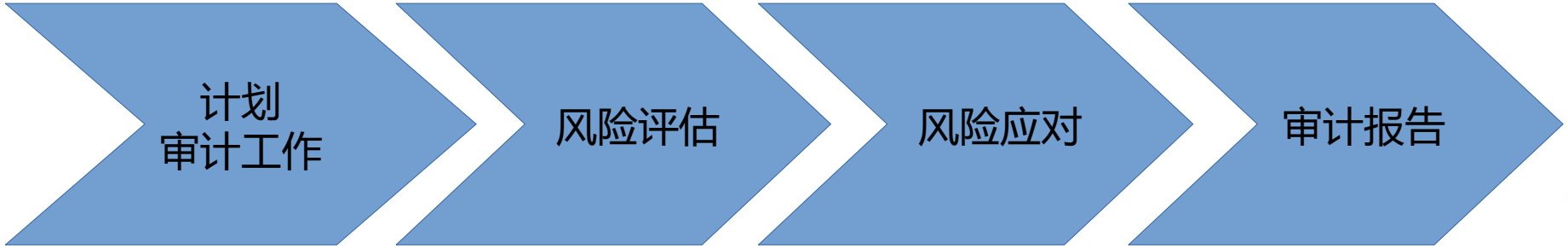
- 一道防线：业务部门是风险的承担者，应持续识别、评估和报告风险。
- 二道防线：风险管理部门和合规部门是第二道风险防线。风险管理部门负责监督和评估业务部门承担风险的业务活动。
- 三道防线：内部审计对风险治理框架质量和有效性进行审计。
- 在银行内部构造出三个对风险管理承担不同职责的团队或管理部门，相互之间协调配合，分工协作，并通过独立、有效地监控，提高主体的风险管理有效性。

区块链基础设施的 IT 审计

- 内部审计是一个大的范围，我们在这里主要讨论区块链基础设施的 IT 审计，以及 IT 技术专家在审计团队中的作用。
- 充分考虑审计覆盖面与监管要求，确保合规。主要依据是《金融分布式账本技术安全规范》。
- 分析以前年度审计发现的问题和内控评价情况、生产事件和安全事件发生情况，以及一、二道防线综合评价情况。
- 从外部或一道防线的业务部门，“借调”区块链技术专家到审计团队。专家负责解答各级 IT 审计人员项目执行过程中遇到的具体问题，注意从审计角度考虑问题。

审计常见流程

- 区块链技术专家的工作，贯穿审计主线。
- 每年初，依据法规，结合区块链基础设施的情况，修订《审计方法》，更新审计对象库。负责解答各级 IT 审计人员项目执行过程中遇到的具体问题。



文本分析《安全规范》

单词	词频
节点	259
身份	195
账本	140
合约	119

文本分析《安全规范》

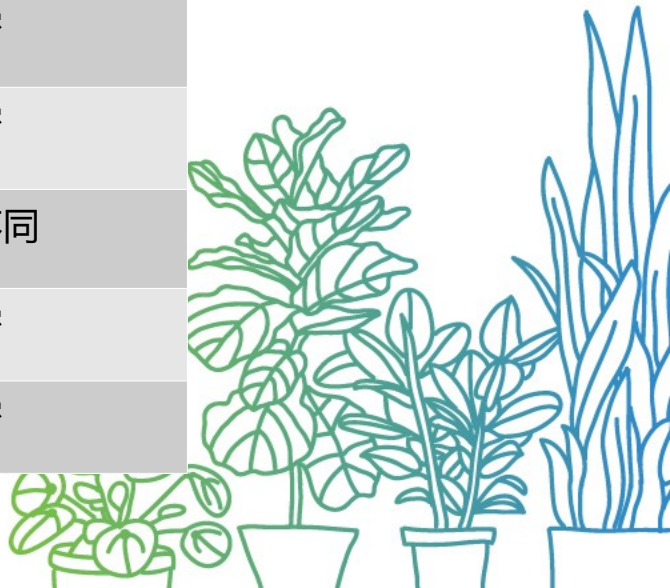
单词	词频
安全	98
交易	96
凭证	84
审计	73
共识	66
分布式	64
密钥	56
存储	56
标识	55

文本分析《安全规范》

单词	词频
授权	48
隐私	46
权限	45
算法	42
验证	42
注册机构	40
证书	39
策略	35
区块	27

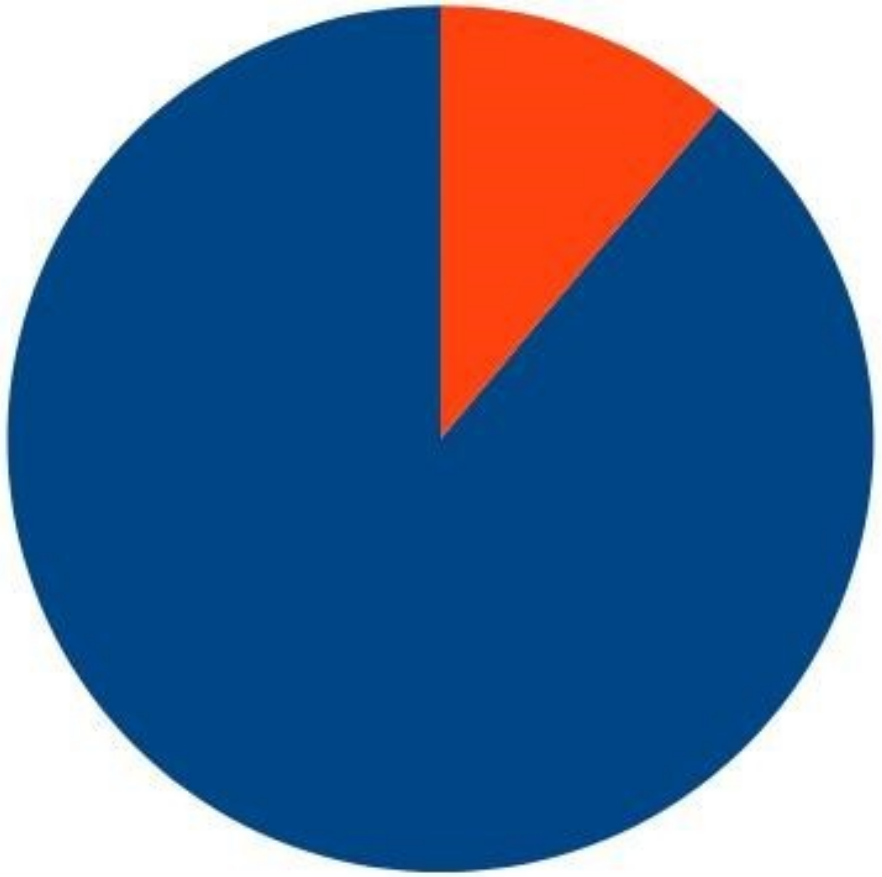
需要关注的《安全规范》项目

条目	结论	类型
6.2.4 硬件加密设备安全符合国密 GM/T 0045—2016	不满足	不支持国密
7.8 数据传输	不满足	不支持国密
8.1 密码算法 基本要求条款指定符合国密标准	不满足	不支持国密
8.6 随机性 密码算法随机数，符合 GB/T 32915—2016	不满足	不支持国密
9.3 通信完整性 符合国密的完整性保护和校验	不满足	不支持国密
9.4 通信保密性 采用国密生成密钥，建立安全信道。	不满足	不支持国密
11.4 终局性 所有节点，最终达成一致。	不满足	架构设计不同
13.8 节点标识管理 符合第 8 章“密码算法”要求	不满足	不支持国密
13.10.3 安全加密 符合国密 GM/T 0045—2016	不满足	不支持国密



HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

不满足《安全规范》的类型



例一：风险评估矩阵

序号	评估项	模块	法规依据	评估结果	备注
1	硬件加密设备应满足如下要求： - 使用的加密机设备应符合国家密码管理部门颁布的GM/T 0045—2016的要求； - 使用的个人密码设备（如UKey、加密卡、带SE或TEE的移动终端等）应符合行业主管部门和国家密码管理部门的要求。	基础硬件	《安全规范》6.2.4 硬件加密设备安全	不通过	fabric 此种要
	共识模块应能协调各系统参与方有序参与数据打包和共识过程，并保证各参与方的数据一致性	基础软件	《安全规范》7.3 共识模块	通过	fabric solo、 机制，

例二：安全配置项的建议

```
    grpc:
      port: 7054
peers:
- peer:
  name: peer0
  type: anchor    # This can be anchor/nonanchor.
  gossippeeraddress: peer0.warehouse-net:7051 # I
  peerAddress: peer0.warehouse-net.org3ambassador
  certificate: "/path/ca.crt" # certificate path
  cli: disabled      # Creates a peer cli pod dep
  grpc:
    port: 7051
  events:
```

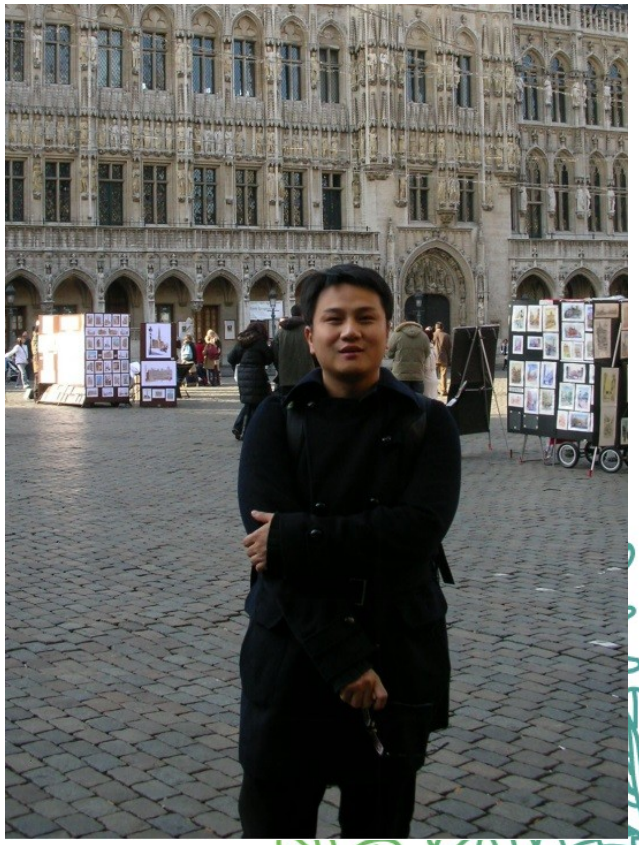
依据安全配置项的建议，进行重点检查。如有必要，邀请外部安全团队介入。

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

作者介绍

Terry 万勇

Hyperledger TWG 中国工作组志愿者、前 IBMer，曾任 IBM 中国创新中心“2017 创新实验室 -IBM 中国大学合作”项目的导师，致力于新技术在国内的推广宣传。现在是一名自由职业者，热心参与开源社区活动，专注于区块链技术的进展和项目落地。



HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

参考文献

- 《金融分布式账本技术安全规范》（JR/T 0184—2020）中国人民银行
- 《商业银行信息科技审计研究与实践》中国金融科技风险管理及审计最佳实践

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

答疑和讨论 Q&A