ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33863.2—2017/IEC/TR 62541-2:2010

OPC 统一架构　第 2 部分:安全模型

OPC unified architecture—Part 2: Security model

(IEC/TR 62541-2:2010,IDT)

2017-07-12 发布　　2018-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 33863《OPC 统一架构》由以下各部分组成：

——第 1 部分：概述和概念；

——第 2 部分：安全模型；

——第 3 部分：地址空间模型；

——第 4 部分：服务；

——第 5 部分：信息模型；

——第 6 部分：映射；

——第 7 部分：规约；

——第 8 部分：数据访问；

——第 9 部分：报警和条件；

——第 10 部分：程序；

——第 11 部分：历史访问；

——第 12 部分：发现；

——第 13 部分：聚合。

本部分是 GB/T 33863 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用 IEC/TR 62541-2:2010《OPC 统一架构　第 2 部分：安全模型》。

本部分做了下列编辑性修改：

——删除与规范性引用文件重复的参考文献。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、北京三维力控科技有限公司、上海自动化仪表有限公司、重庆川仪自动化股份有限公司、西南大学、中国工程物理研究院动力部。

本部分主要起草人：王麟琨、王春喜、李云、丁露、王玉敏、丁研、张庆军、姚杰、刘枫、郑秋平。

引　言

本部分为GB/T 33863规定的OPC统一架构提供了安全模型。本标准给出了为开发标准接口而进行分析和设计的过程，该标准接口可加快由多个供应商完成的应用开发，并实现内部操作的无缝连接。

OPC 统一架构　第 2 部分:安全模型

1　范围

GB/T 33863 的本部分给出了 OPC 统一架构(UA)安全模型,描述了 OPC UA 预期要运行的物理、硬件和软件环境中的安全威胁,以及 OPC UA 如何利用其他标准实现安全。本部分给出了在 OPC UA 其他规范中规定的安全特性的概述。本部分引用了在本标准其他部分做了规范性规定的服务、映射和行规。

注:在开发应用时,需解决安全性的许多其他方面。鉴于 OPC UA 规定了一个通信协议,所以本部分关注于保护应用间数据交换的安全。

这并不意味着应用开发者可以忽略其他方面的安全,如保护永久性数据免遭篡改。开发者应观察所有安全内容,并确定在应用中如何处理。

本部分用于指导开发 OPC UA 客户端或服务器应用,或实现 OPC UA 服务层。

本部分假定读者熟悉 Web 服务和 XML/SOAP。关于这些技术的信息,可参考 SOAP 第 1 部分和第 2 部分。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

IEC 62541 (所有部分)　OPC 统一架构(OPC unified architecture)

IEC/TR 62541-1　OPC 统一架构　第 1 部分:概述和概念(OPC unified architecture—Part 1: Overview and concepts)

3　术语、定义、缩略语和约定

3.1　术语和定义

IEC/TR 62541-1 界定的以及下列术语和定义适用于本文件。

3.1.1

应用实例　Application Instance

在一台计算机上运行的一个单独安装的程序。

注:同一应用的几个应用实例可以同时在一台或多台计算机上运行。

3.1.2

应用实例证书　Application Instance Certificate

已安装在单个主机中的单个应用实例的数字证书。

注:一个软件产品的不同安装应有不同的应用实例证书。

3.1.3

非对称密码术　Asymmetric Cryptography

使用一对密钥的加密方法。一个密钥指定为私有密钥,不公开;另一个密钥称为公开密钥,通常可获得。

注：非对称密码术，也称为“公开密钥密码术”。在非对称加密算法中，当实体 A 要确保发给实体 B 数据的保密性时，实体 A 使用实体 B 提供的公开密钥对数据进行加密。只有实体 B 具有解密数据所需的相匹配的私有密钥。在非对称数字签名算法中，当实体 A 要确保发给实体 B 的数据的完整性或要提供数据鉴别时，实体 A 使用其私有密钥对数据进行标记。为验证签名，实体 B 使用实体 A 提供的匹配的公开密钥。在非对称密钥约定算法中，实体 A 和实体 B 相互发送他们的公开密钥。然后每个实体使用其私有密钥和对方的公开密钥计算新密钥值，见 IS 术语表。

3.1.4

非对称加密　Asymmetric Encryption

非对称密码术使用的一种机制，该机制使用一个实体的公开密钥加密数据，使用相关联的私有密钥解密数据；

注：详见 3.1.3。

3.1.5

非对称签名　Asymmetric Signature

非对称密码术使用的一种机制，该机制使用实体的私有密钥标记数据，并使用相关联的公开密钥验证数据签名。

注：详见 3.1.3。

3.1.6

可审核性　Auditability

确保系统中任何行为或活动可被记录的一种安全目标。

3.1.7

审核　Auditing

对系统内的行为和活动，包括安全相关活动，进行跟踪。其中，审核记录可被用于验证系统运行的安全性。

3.1.8

鉴别　Authentication

验证实体(如：客户端、服务器或用户)特征的过程。

3.1.9

授权　Authorization

授予系统实体访问系统资源的权利或许可的过程。

3.1.10

可用性　Availability

系统无阻碍运行的能力。

3.1.11

机密性　Confidentiality

保护数据避免被非预期的实体读取。

3.1.12

密码术　Cryptography

使用算法和密钥将清晰、有含义的信息变换为加密的难以理解的格式。

3.1.13

网络安全管理系统　Cyber Security Management System；CSMS

由某个组织设计的程序，以维护整个组织资产安全达到确定的机密性、完整性和可用性的等级。资产可以属于该组织的商业范畴也可以属于该组织的工业自动化和控制系统范畴。

3.1.14

数字证书　Digital Certificate

将特征与一个实体(如:用户、产品或应用实例)相关联的结构,该证书有一个相关联的非对称密钥对,可用于鉴别该实体确实拥有私有密钥。

3.1.15

数字签名　Digital Signature

使用加密算法计算并附加到数据上的值。任何数据接收可使用该签名验证数据的来源和完整性。

3.1.16

散列函数　Hash Fnction

一种算法,如 SHA-1,对于该算法,寻找映射到给定散列结果("单向"属性)的一个数据对象或寻找映射到同一散列结果的两个数据对象("无碰撞"属性)在计算上是不可行的,见 IS 术语表。

3.1.17

散列消息鉴别码　Hashed Message Authentication Code;HMAC

使用迭代散列函数生成的 MAC(消息鉴别码)。

3.1.18

完整性　Integrity

保证在未授权情况下不修改或不损坏信息的安全目标。

注:定义来自 IS 术语表。

3.1.19

密钥交换算法　Key Exchange Algorithm

用于在不安全环境下的两个实体间建立安全通信路径的协议,两个实体使用特定算法安全地交换用于保证彼此间安全通信的密钥。

注:密钥交换算法的一个典型实例是在 SSL/TLS 中规定的 SSL 握手协议。

3.1.20

消息鉴别码　Message Authentication Code;MAC

使用密钥(见对称加密)来散列计算消息的算法所产生的短数据片。由此消息接收者能通过计算 MAC 来检查消息是否发生变化。使用相同消息和密钥,MAC 应相同。

3.1.21

消息签名　Message Signature

用于保证在两个实体间发送消息完整性的数字签名。

注:有多种方法来产生和验证消息签名,这些方法可以分为对称方法(见 3.1.32)和非对称方法(见 3.1.5)。

3.1.22

不可否认性　Non-Repudiation

证明消息签名者标识和消息完整性的证据是有力而充分的,以避免对方否认报文的原传输或传递,以及内容的完整性。

3.1.23

Nonce

通常由产生安全密钥的算法使用一次的随机数。

3.1.24

OPC UA 应用　OPC UA Application

调用 OPC UA 服务的 OPC UA 客户端或执行这些服务的 OPC UA 服务器。

3.1.25

私有密钥　Private Key

用于非对称加密的一对加密密钥的保密部分。

3.1.26

公共密钥　Public Key

用于非对称加密的一对加密密钥的可公开部分，见 IS 术语表。

3.1.27

公共密钥基础设施　Public Key Infrastructure;PKI

产生、管理、存储、分发和取消基于非对称加密的数字证书所需要的硬件、软件、人员、策略和规程集。

注：核心 PKI 功能是注册用户、发布公共密钥证书、在需要时取消证书以及在延迟时间很长时对确认证书所需的数据进行存档。保证数据机密性的密钥对可由证书认证机构(CA)产生，但要求私有密钥所有者产生自身的密钥对以提高安全性，因为绝不会传输私有密钥，见 IS 术语表。公共密钥结构的更多细节见 PKI 和 X509 PKI。

3.1.28

Rivest-Shamir-Adleman，RSA

非对称密码术，由 Ron Rivest，Adi Shamir 和 Leonard Adleman 于 1977 年发明，见 IS 术语表。

3.1.29

安全通道　Secure Channel

在 OPC UA 客户端和服务器之间建立的通信路径。OPC UA 客户端和服务器已使用确定的 OPC UA 服务相互进行鉴别，通信路径的安全参数通过协商方式确定并使用。

3.1.30

对称密码术　Symmetric Cryptography

一种加密技术，这种技术使用的算法在两个不同步骤中使用相同密钥(例如：加密和解密，或产生签名和签名验证)，见 IS 术语表。

3.1.31

对称加密　Symmetric Encryption

由对称密码术使用的机制，该机制使用由两个实体共享的加密密钥对数据进行加密和解密。

3.1.32

对称签名　Symmetric Signature

由对称密码术使用的机制，该机制使用两个实体共享的密钥对数据进行签名。

注：通过再次产生数据签名并比较这两个签名，对数字签名进行确认。如果相同则数字签名有效，否则两个实体的密钥或数据不同。3.1.17 定义了生成对称密钥算法的典型示例。

3.1.33

X.509 证书　X.509 Certificate

符合 X.509 v1、2 或 3 中所定义的一种格式的数字证书。

注：X.509 证书包含数据项序列，以及基于此序列计算得到的数字签名。

3.2　缩略语

下列缩略语适用于本文件。

CSMS：网络安全管理系统(Cyber Security Management System)

DSA：数字签名算法(Digital Signature Algorithm)

PKI：公共密钥基础设施(Public Key Infrastructure)

RSA：用于签名或加密的公共密钥算法(Rivest，Shamir，Adleman)[public key algorithm for signing or encryption(Rivest，Shamir，Adleman)]

SHA1：安全散列算法 1(Secure Hash Algorithm 1)

SOAP：简单对象访问协议(Simple Object Access Protocol)

SSL:安全套接层(Secure Sockets Layer)
TLS:传输层安全(Transport Layer Security)
UA:统一架构(Unified Architecture)
URI:统一资源标识符(Uniform Resource Identifier)
XML:可扩展标记语言(Extensible Mark-up Language)

3.3 关于安全模型图的约定

本部分的图不使用任何特定共用约定,在特定图中使用的任何约定仅用于解释该图。

4 OPC UA 安全结构

4.1 OPC UA 安全环境

OPC UA 是对工业设施在多层次操作过程中组件间使用的协议,多层次操作过程涵盖上层企业管理到对底层设备的直接过程控制。使用 OPC UA 用于企业管理涉及客户和供应商,对于工业间谍或破坏者它可能是有吸引力的目标,也可能处于在公共网络上活动的无目的的恶意软件的威胁之下,如“蠕虫”。过程控制端的通信中断至少会提高企业的经济成本,并且可带来雇员和公共安全后果,或造成环境危害。这对于寻找机会危害企业或社会的人来说可能是有吸引力的目标。

OPC UA 将应用在不同类型的工作环境中,对于不同的工作环境应对威胁和可访问采用不同假设,以及使用不同安全策略和强制制度。因此,OPC UA 提供了一套灵活的安全机制集。图 1 给出了这些不同环境的组合。一些 OPC UA 客户端和服务器在相同主机上,能更容易地避免外部攻击。一些客户端和服务器在相同工作网络上的不同主机上,可通过安全边界保护避免外部攻击,安全边界保护将工作网络与外部连接隔离。一些 OPC UA 应用在相对开放的环境下运行,在这样环境下用户和应用可能难以控制。其他应用嵌入到控制系统中,这些控制系统与外部系统没有直接的电子连接。

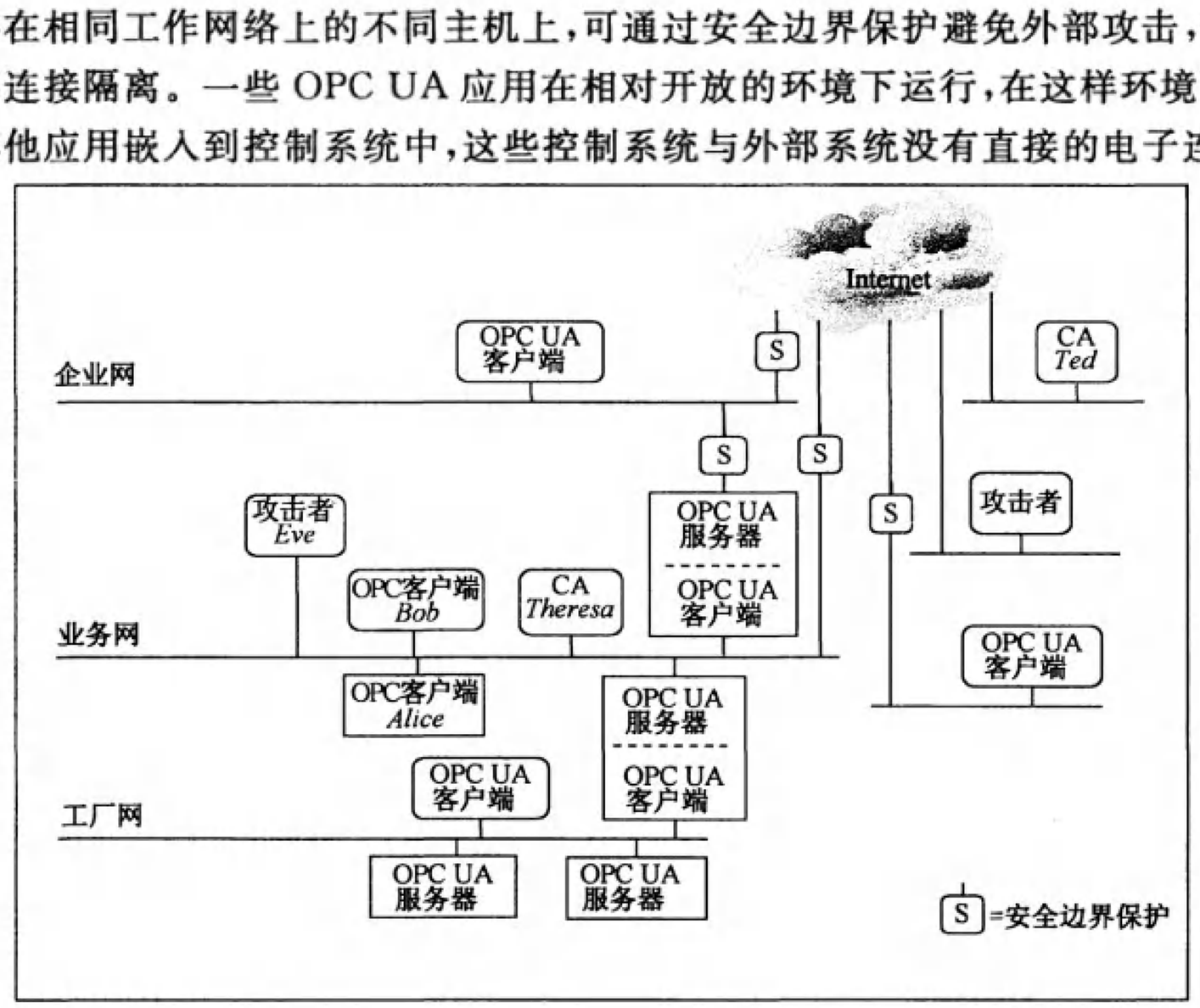

图 1 OPC UA 网络模型

OPC UA 应用可能运行在不同环境中的不同地点。客户端和服务器可能在高防护控制网络上的相同主机或主机间通信。但 OPC UA 客户端和服务器也可能在因特网上很开放的环境下通信。站点向 OPC UA 应用运行的系统部分提供的任何安全控制保护,可保护 OPC UA 活动。

4.2 安全目标

4.2.1 概述

信息系统安全从根本上降低了攻击造成危害的风险,可通过识别对系统的威胁、识别系统对这些威胁的弱点、以及提供相应对策来实现。这些对策直接减少了系统的弱点、阻止了威胁,或从成功的攻击中恢复。

工业自动化系统的安全通过满足目标集来实现。通常为信息系统提供安全的这些目标经过长期经验已经得到了改进。尽管对系统的威胁不断变化,但目标集保持较高稳定性。这些目标在后续条中描述。在描述 OPC UA 安全结构和功能之后,5.2 根据 OPC UA 功能协调这些目标。

4.2.2 鉴别

像客户端、服务器和用户这样的实体,应检验其标识。鉴别可基于实体已有和已知的知识实现。

4.2.3 授权

对读、写或执行资源的访问仅应授权给该系统要求范围内的需要这种访问的实体。授权可以是粗粒度的,允许或不允许客户端调用服务器,也可以是细粒度,如允许特定用户对特定信息的特定动作。

4.2.4 机密性

无论数据在传输过程中、在存储器中还是在存储过程中,都应保护数据避免被动攻击,如窃听。为提供机密性,使用保护数据的特定保密机制的数据加密算法应与访问该保密机制的鉴别和授权机制一同使用。

4.2.5 完整性

接收器应接收与发送器发送的相同的信息,在传输过程中数据不被改变。

4.2.6 可审核性

为了给利益相关者提供该系统按预期工作的证据以及识别某些动作的发起者,应记录系统采取的动作。

4.2.7 可用性

当需要执行的软件被关闭或当正在处理的输入超过了软件或通信系统自身能力,则可用性被降低。OPC UA 可用性降低表现为:例如,订阅性能下降或增加会话的能力下降。

4.3 对 OPC UA 系统的安全威胁

4.3.1 概述

OPC UA 提供措施以阻止对传送信息安全的威胁。后面条列出了当前已知的对 OPC UA 运行环境的威胁,描述了 OPC UA 安全结构和功能。5.1 给出了如何解决对 OPC UA 功能的威胁。

4.3.2 消息洪泛

攻击者发送大量的消息,或一个包含大量请求的消息,以达到使 OPC UA 服务器或 OPC UA 服务器可靠工作所依赖的部件(如:CPU,TCP/IP 栈、操作系统或文件系统)难以应付。洪泛攻击可在多层实施,包括 OPC UA、SOAP、[HTTP]或 TCP。

消息洪泛攻击可使用格式正确消息和畸形消息。

第一个场景:攻击者是一个使用合法客户端的恶意者,向服务器发送不间断的请求。存在两种情况,一种情况客户端与服务器没有会话,另一种情况是有会话。消息洪泛可能对建立 OPC UA 会话的能力造成损害,或终止已建立的会话。

第二个场景:攻击者使用恶意客户端向 OPC UA 发送大量畸形消息,以达到耗尽服务器资源的目的。

通常消息洪泛可能消弱与 OPC UA 实体的通信能力,并导致拒绝服务。

消息洪泛可影响可用性。

该威胁的处理见 5.1.2。

4.3.3 窃听

窃听是未经授权的披露敏感信息,这可直接导致严重安全破坏或用于后续攻击。

如果攻击者威胁到底层操作系统或网络结构的安全,攻击者可能已经记录并捕获了消息。恢复受损的操作系统不在客户端或服务器的能力范围内。

窃听直接影响机密性并间接影响其他所有安全目标。

该威胁的处理见 5.1.3。

4.3.4 消息欺骗

攻击者可以伪造来自客户端或服务器的消息,欺骗可能发生在协议栈的多层。

通过伪造来自客户端或服务器的消息,攻击者可执行未授权的操作,并避免其行为被侦测。

消息欺骗影响完整性和授权。

该威胁的处理见 5.1.4。

4.3.5 消息改变

网络数据流和应用层消息可被捕获、修改,修改后的消息被转发给 OPC UA 客户端和服务器。消息改变可能允许对系统进行非法访问。

消息改变影响完整性和授权。

该威胁的处理见 5.1.5。

4.3.6 消息重放

网络数据流和有效的应用层消息被捕获并滞后一段时间后无修改地重新发送给 OPC UA 客户端和服务器。攻击者可向用户通知错误消息或发送不合适的命令,例如:在不合适的时间发送打开阀门的命令。

该威胁的处理见 5.1.6。

4.3.7 畸形消息

攻击者能构造多种带有无效消息结构(畸形的 XML、SOAP、UA 二进制等)的消息或数据值,并将其发送给 OPC UA 客户端或服务器。

通过执行未授权的操作或处理不必要信息,OPC UA 客户端或服务器可能错误处理某些畸形消息。这可能导致拒绝服务或服务降级,包括终止应用或嵌入式设备的崩溃。在最糟糕场景下攻击者可能也使用畸形消息作为多层次攻击的预备阶段,以获取对 OPC UA 应用底层系统的访问。

畸形消息影响完整性和可用性。

该威胁的处理见 5.1.7。

4.3.8 服务器剖析(profiling)

攻击者尝试推导出服务器或客户端的标识、类型、软件版本或供应商,以便将有关该产品特定脆弱性的知识用于实施更有侵略性或更有危害性的攻击。攻击者可能通过向目标发送有效或无效格式的消息来剖析目标,并尝试通过正常和错误响应的模式来识别目标类型。

服务器剖析间接影响所有安全目标。

该威胁的处理见 5.1.8。

4.3.9 会话劫持

攻击者可能使用在两个应用间建立的运行会话的信息(通过嗅探通信或猜测获得),以插入伪造消息(带有有效会话消息),这允许攻击者接管已授权用户的会话。

攻击者可能对数据进行未授权访问,或执行未授权操作。

会话劫持影响所有目标。

该威胁的处理见 5.1.9。

4.3.10 欺诈服务器

攻击者建立恶意 OPC UA 服务器或安装未授权的真正的 OPC UA 服务器实例。

该 OPC 客户端可能透露必要信息。

欺诈服务器影响除完整性以外的所有安全目标。

该威胁的处理见 5.1.10。

4.3.11 用户凭证泄密

攻击者通过观察纸质文件、屏幕或电子通信来获取用户凭证,如:用户名、密码、证书或密钥,或通过猜测或使用自动工具(如密码破解器)来获取用户凭证进行破解。

未授权用户可以启动和访问系统,以获取所有信息并执行控制和修改数据,这会对工厂操作或工厂信息造成损害。一旦使用泄密凭证,后续活动可能表现为合法。

用户凭证泄密影响授权和机密性。

该威胁的处理见 5.1.11。

4.4 OPC UA 与站点安全的关系

OPC UA 安全在站点的整个网络安全管理系统(CSMS)范围内工作。站点通常有描述安全策略、规程、人员、责任、审核和物理安全的 CSMS。CSMS 通常会描述威胁,包括在 4.3 中描述的威胁。CSMS 也分析了安全风险并确定站点需要的安全控制。

因此而产生的安全控制通常实现“深度防御”策略,这种策略提供多层防护并认为单层不能防护所有的攻击。边界保护,在图 1 中所示的抽象示例,可包括防火墙入侵侦测和防护系统、拨入连接控制、系统内的介质控制和计算机控制。系统内部件的保护可包括操作系统的固化配置、安全补丁管理、杀毒程序和不允许在控制网络使用电子邮件(email)。站点可参照的标准包括 NERC CIP 和 IEC 62351,见参考文献。

站点 CSMS 的安全要求适用于其 OPC UA 接口。即:站点使用的 OPC UA 接口的安全要求由该站点规定,而不是由 OPC UA 规范规定。OPC UA 规定了客户端和服务器产品应具备的特性,使其能满足所在的站点给出的预期安全要求。站点内负责安全的人员应确定如何使用 OPC UA 一致性产品满足站点要求。

安装 OPC UA 客户端或服务器的系统所有者应该分析安全风险并提供适合的机制,以降低风险达

到可接受的安全等级。OPC UA 满足多种不同的安全需要，这些需要可能来自不同的独立分析的结果。这就要求 OPC UA 客户端和服务器实现某些安全特性，这些安全特性可供系统所有者选择使用。每个系统所有者通过联合使用 OPC UA 规范和规范外可用的机制，应能定制出满足其安全和经济要求的安全解决方案。

对站点内使用的 OPC UA 客户端和服务器的安全要求由站点 CSMS 规定，不是由 OPC UA 规范规定。OPC UA 安全规范是对 OPC UA 客户端和服务器产品的要求，也是建议 OPC UA 应在站点如何使用以满足站点规定的预期的安全要求。

OPC UA 要处理的威胁在 4.3 中描述。OPC 基金会推荐制造商按第 6 章规定处理残余威胁。可能危及客户端和服务器操作系统安全的对底层组件的威胁，不在 OPC UA 处理的范围内。

4.5 OPC UA 安全架构

OPC UA 安全架构是允许在 OPC UA 应用结构中不同地点实现要求的安全特性的通用解决方案。根据在 IEC 62541-6 描述的不同映射，安全目标可在不同层次实现。OPC UA 安全架构被构建在传输层之上的应用层和通信层中，见图 2。

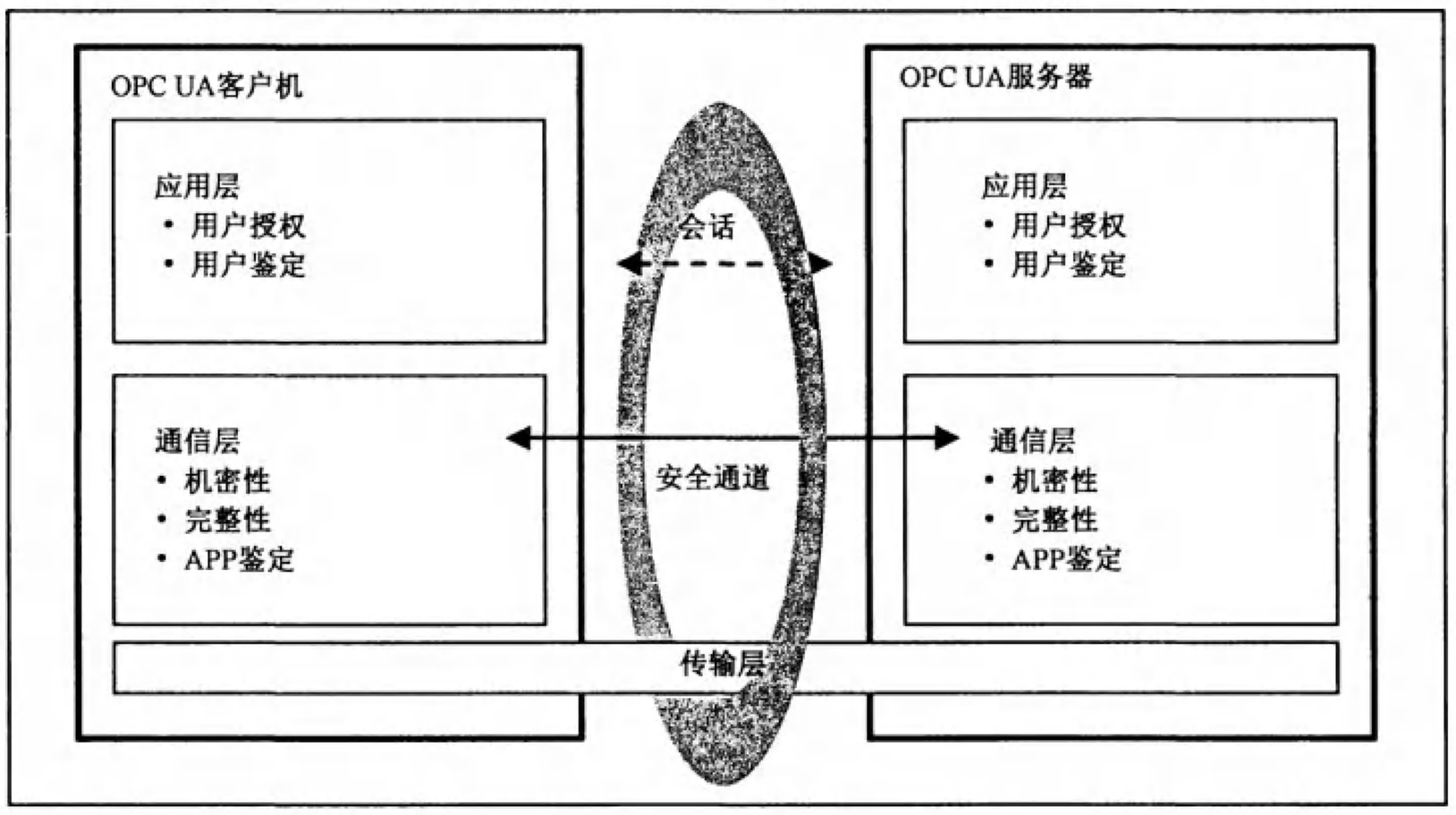

图 2 OPC UA 安全架构

客户端应用和服务器应用传输工厂信息、设置和命令这些日常工作在应用层的会话阶段完成。应用层通过用户鉴别和用户授权管理安全目标。由应用层管理的安全目标由 IEC 62541-4 规定的会话服务处理。应用层的会话在安全通道上通信并依靠安全通道实现安全通信，安全通道由该通信层产生。所有的会话数据传递给通信层做进一步处理。

尽管会话通信在安全通道上实现并在使用前必须被激活，但可灵活对用户、会话和安全通道进行绑定。

允许改变会话的用户。鉴于在激活会话之前用户凭证是无效的，因此会话的用户可与第一次激活会话的用户不同。

当安全通道断开时，在会话有效期内会话仍为有效，可重新建立安全通道，否则在会话有效期期满后，会话将关闭。

通信层提供安全机制以实现作为安全目标的机密性、完整性和应用鉴别。

满足上述安全目标的一个关键机制是建立安全通道（见 4.11），用于保障客户端和服务器之间通信的安全。安全通道提供加密以维护机密性，提供消息签名以维护完整性，提供数字证书为来自应用层的

数据提供应用鉴别，并将该“安全”数据传递到传输层。由通信层管理的安全机制通过 IEC 62541-4 规定的安全通道服务来提供。

由安全通道服务提供的安全机制由实现选择的协议栈提供。在 IEC 62541-6 中规定了这些服务到某些协议栈选项的映射，在该部分详细叙述了怎样使用协议栈功能来实现 OPC UA 安全目标。

通信层能表示 OPC UA 协议栈，OPC UA 规定了可用作通信层的 2 个可选的协议栈映射，分别是：OPC UA 固有映射和网页服务映射。

如果使用 OPC UA 固有映射，则机密性功能、完整性、应用鉴别和安全通道与 IEC 62541-6 中描述的 SSL/TLS 规范相似。

如果使用 Web 服务映射，则 WS 安全、WS 安全转换、XML 加密，以及 XML 签名被用于实现机密性、完整性、应用鉴别，以及实现安全通道机制，详见 IEC 62541-6。

传输层处理发送、接送和传输通信层提供的数据。

为恢复已断开的传输层连接(例如：TCP 连接)，通信层实现负责重新建立传输层连接，而不中断逻辑安全通道。

4.6 安全策略

安全策略规定了使用哪种安全机制以及派生它们的安全行规(详见 4.7)。服务器使用安全策略宣布其支持的机制，客户端使用安全策略选择其中一个可用策略用于希望打开的安全通道。规定的安全策略包括：

——签名和加密算法；

——密钥推导算法。

通常由控制系统管理者在客户端和服务器产品已安装后，选择安全策略。

通报安全策略由 IEC 62541-4 规定的特定安全发现服务处理。更多发现机制和策略通报见 IEC 62541-12。

如果服务器服务多个客户端，该服务器为不同客户端维护多个不同的策略选择。这允许新客户端在选择策略时，无需考虑其他客户端为其安全通道已选择的策略。

鉴于每经过几年计算能力都会获得较大增强，现在认为是安全的特定算法在将来会成为不安全，所以在 OPC UA 应用中支持多种安全策略是必要的，这使得在上述情况下能改进其安全策略。

也存在这样的情况，新安全策略被调整以支持可提高 OPC UA 产品安全性等级的新算法。OPC UA 客户端和服务器的应用结构设计宜可以为应用更新或添加附加加密算法。

IEC 62541-7 规定了由特定惟一 URI 标识的几个策略。为提高制造商产品的互操作性，服务器产品应实现这些策略而不是定义自己的策略。

4.7 安全行规

OPC UA 客户端和服务器产品根据 IEC 62541-7 定义的行规对产品进行认证。一些行规规定了安全功能，还有其他行规规定了与安全无关的其他功能。行规对认证产品提出了要求，但行规不会给出关于如何使用产品的要求。不同行规要求一致的最低安全等级。但不同行规规定了不同细节，如不同 OPC UA 功能要求不同加密算法。如果在一个加密算法中发现了一个问题，则 OPC 基金会会定义新的相似行规，新行规规定了不存在已知问题的不同加密算法。IEC 62541-7 是关于行规的规范性规范。

策略参考了许多与行规相同的安全选择，然而，策略规定在会话中使用哪种选择。策略与行规不同，策略不规定产品提供的选择范围。

OPC UA 的每个安全机制由符合相应行规的客户端或服务器提供。站点可以随意地选择使用的安全机制。按此方式每个单个站点具有所有可用的 OPC UA 安全功能，并能决定选择使用哪种功能以满足其安全目标。

4.8 用户授权

OPC UA 提供一种机制以交换用户凭证但未规定应用如何使用这些凭证。客户端和服务器应用可以按自己的方式确定什么数据是可访问的,以及什么操作被授权。

4.9 用户鉴别

用户鉴别由会话服务提供,客户端可使用会话服务传递用户凭证给服务器,见 IEC 62541-4。服务器能使用这些凭证鉴别客户。

可使用 ActivateSession 服务改变正通过会话进行通信的用户,以满足应用需求。

4.10 应用鉴别

OPC UA 使用传送应用鉴别的方法,以允许打算进行通信的应用相互识别。每个 OPC UA 应用实例有一个分配的数字证书(应用实例证书),在安全通道建立期间交换该证书。证书接收者检查该证书是否值得信任,基于检查结果,拒绝来自发送者的请求或给出响应消息。

关于应用鉴别的更详细信息见 IEC 62541-4。

4.11 OPC UA 安全相关服务

OPC UA 安全服务是 IEC 62541-4 中规定的一组抽象服务定义。安全服务用于将不同安全机制应用于 OPC UA 客户端和服务器之间的通信。

发现服务集(见 IEC 62541-4)定义了 OPC UA 客户端使用的服务,以通知安全策略(见 4.6)和特定 OPC UA 服务器的数字证书。

安全通道服务集中的服务用于建立安全通道,安全通道负责在客户端和服务器之间发送安全消息。建立安全通道的挑战是要求客户端和服务器在不安全环境下安全地交换加密密钥和机密信息,所以通信参与者使用特定密钥交换算法(与 SSL/TLS 定义的 SSL 握手协议相似)。

OPC UA 客户端通过上面描述的发现服务找回安全策略和 OPC UA 服务器的数字证书。这些数字证书包含 OPC UA 服务器的公共密钥。

OPC UA 客户端使用 OpenSecureChannel 服务报文向服务器发送数字证书中的公共密钥和机密信息。通过使用服务器的公共密钥的非对称加密术和使用客户端私有密钥产生非对称签名,来保护消息。但数字证书发送未加密,因此接收器可以使用该证书来验证非对称签名。

服务器使用其私有密钥解密该消息,并使用客户端公共密钥验证非对称签名。OPC UA 客户端的机密信息和服务器的机密信息被用于导出保护所有消息的加密密钥集。此外,使用对称加密术和对称签名,而不是使用非对称方法保护所有其他服务消息。

服务器向客户端发送位于服务响应中的机密信息,客户端能导出相同的加密密钥集。

鉴于客户端和服务器有相同的加密密钥集,客户端和服务器彼此间能以安全方式进行通信。

这些推导的加密密钥周期性地变化,所以攻击者不会拥有无限的时间和不受限的消息序列来确定密钥。

4.12 审核

4.12.1 概述

客户端和服务器产生成功和不成功连接请求、安全选项协商结果、配置改变、系统变化和会话拒绝的审核记录。

OPC UA 通过两种机制为安全审核跟踪提供支持。首先它提供客户端和服务器审核日志的可溯

源性。客户端为包括一个请求的操作产生审核日志输入项。当客户端发出服务请求时,客户端产生审核日志输入项,并将日志输入项的本地标识符加入到发送给服务器的请求中。服务器记录它接收的请求并将客户端输入项 id 包含在其审核日志输入项中。在这种模式下,如果在服务器端侦测到安全相关的问题,相关的客户端审核日志输入项能被定位并检查。OPC UA 不要求审核输入项写入到磁盘,但要求这些输入项可用。OPC UA 为服务器提供产生事件通知的能力,事件通知向能处理和产生日志的客户端报告可审核的事件。关于 OPC UA 服务如何被审核见 IEC 62541-4。

其次,OPC UA 定义了可包含在审核记录中的审核参数,审核参数可提高审核日志和审核事件中的一致性。IEC 62541-5 为这些参数定义了数据类型。其他信息模型可以扩展审核定义。IEC 62541-7 定义了行规,行规包括产生审核事件和使用这些参数,包括客户端审核记录 ID 的能力。

因为审核日志被用于证明系统是安全运行的,因此审核日志本身也应被保护以避免未授权的篡改。如果某人未经授权能修改或删除日志记录,这可能隐藏实际或潜在的安全隐患。因为有许多不同的方法产生和存储审核日志(例如:文件或数据库),所以保护审核日志的机制不在本部分范围内。

后面条给出了支持审核的 OPC UA 服务器和客户端的行为。

4.12.2 单个客户端和服务器

图 3 给出了一个客户端和一个服务器通信的简单示例。

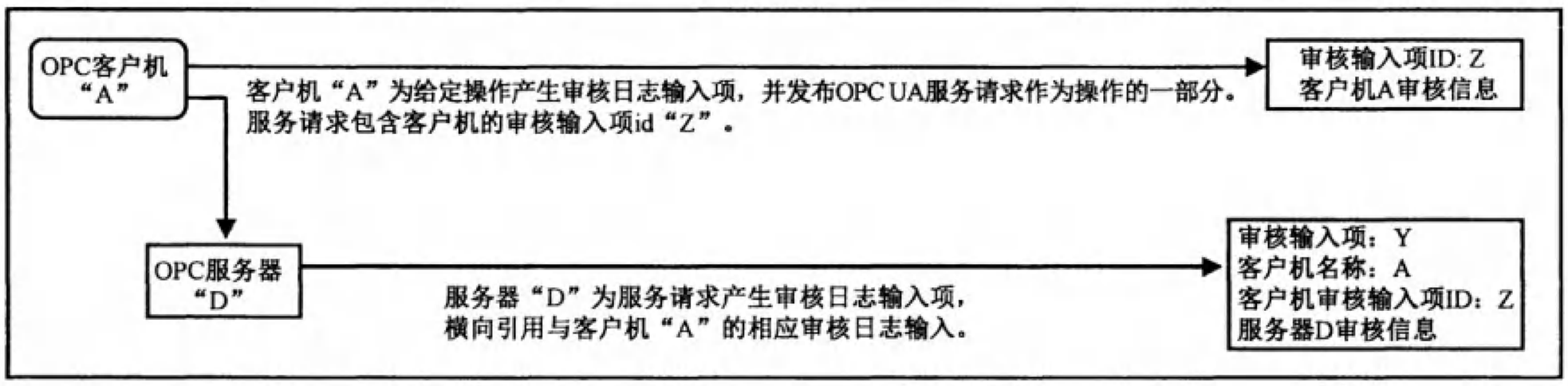

图 3 简单服务器

在这种情况下,客户端“A”执行一些可审核操作,包括在服务器“D”上调用 OPC UA 服务。它写入自己的审核日志输入项,并将该输入项的标识符加入到提交给服务器的服务请求里。

服务器接收该请求并产生自己的审核日志输入项。该输入项通过其自己的审核 ID 来识别,包含自己的审核信息。该输入项也包含发出服务请求的客户端名称和在请求中接收的客户端审核输入项 ID。

使用该信息,审核者能检查服务器日志输入项集,并将其与相关联的客户端输入项关联。

4.12.3 聚合服务器

图 4 给出了客户端访问来自聚合服务器的服务的示例。聚合服务器是通过访问其他 OPC UA 服务器(称为底层服务器)的服务来提供服务的服务器。

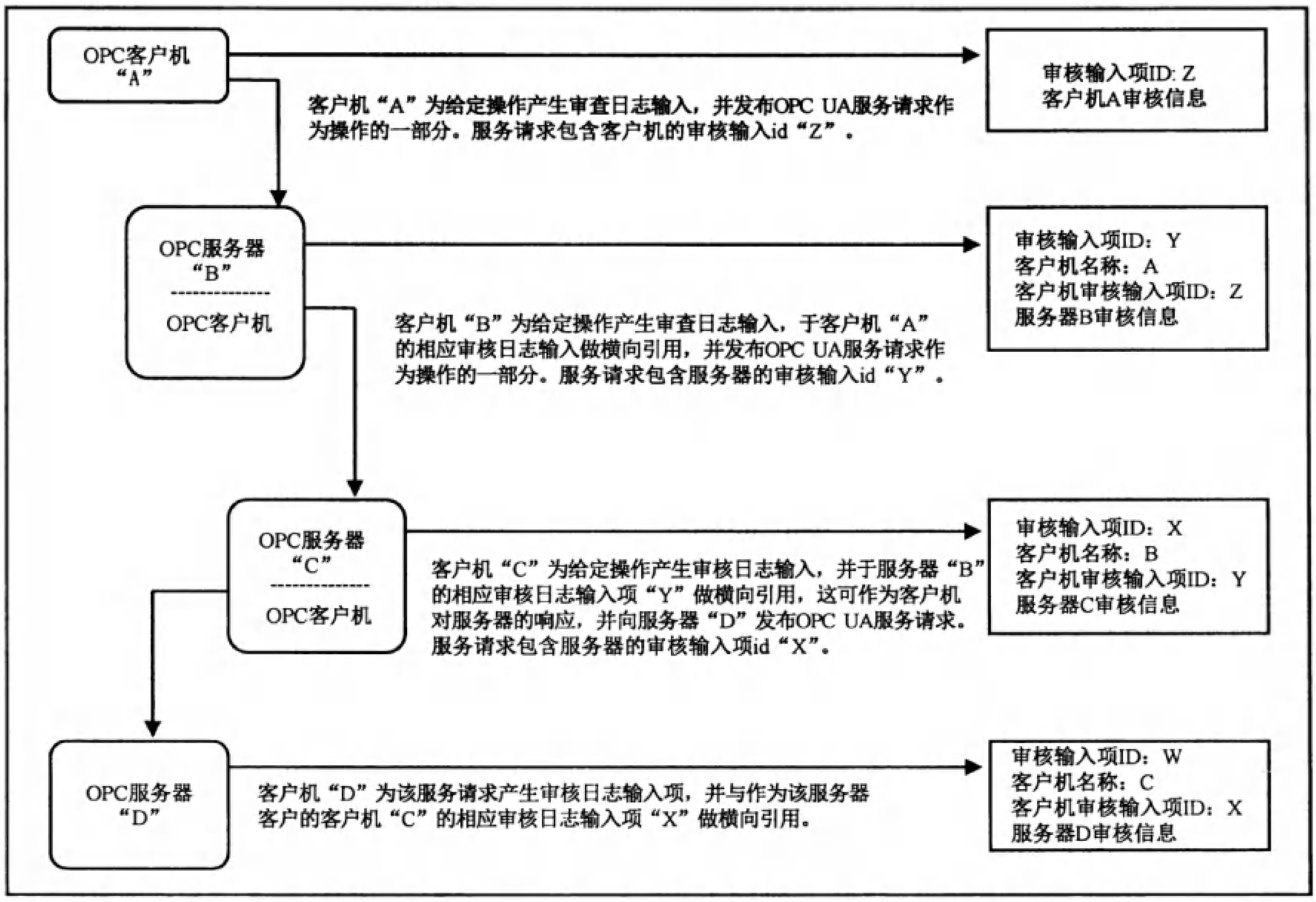

图 4　聚合服务器

在这种情况下，每个服务器接收请求并为其产生自己的审核日志输入项。每个输入项通过其审核ID识别，包含自身的审核信息。该输入项也包含发送服务请求的客户端名称和在请求中接收的客户端审核输入项ID。该服务器将产生的该输入项的审核ID传递给审核链中的下一个服务器。

使用该信息，审核者能检查服务器的日志输入项并将其与相关联的客户端输入项进行关联。

在大多数情况下，服务器将仅产生审核事件，但这些审核事件将仍然包含相同的信息作为审核日志记录。在聚合服务器情况下也要求该服务器向聚合的服务器订阅审核事件。在该模式下，服务器“B”能向客户端“A”提供所有审核事件，包括由服务器“C”和服务器“D”产生的事件。

4.12.4　通过非审核服务器聚合

图5给出了客户端访问来自不支持审核的聚合服务器的服务的示例。

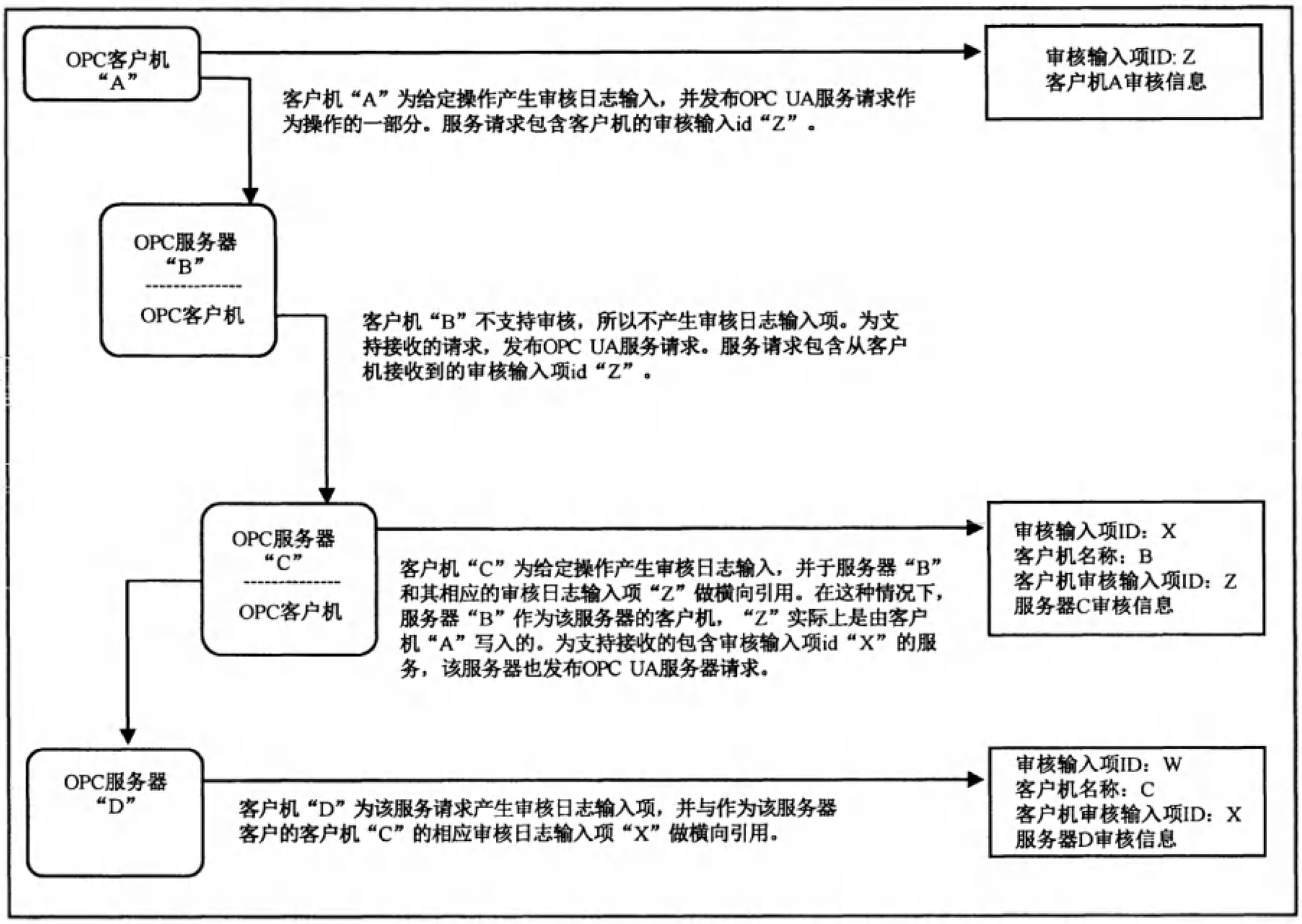

图 5　非审核服务器的聚合

在该情况下，每个服务器接收它们请求并为其产生的审核日志输入项，不支持审核的服务器“B”除外。在此情况下，服务器“B”将它从其客户端“A”接收到的审核 ID 传递给下一个服务器，这将产生所需的审核链。服务器“B”没有列为支持审核的服务器。在服务器不支持写审核输入项的情况下，整个系统可以被认为不支持审核。

在聚合服务器不支持审核情况下，仍要求服务器向聚合的服务器订阅审核事件。在该模型下，尽管服务器“B”不产生审核事件，但服务器“B”应能向客户端“A”提供所有审核事件，包括由服务器“C”和服务器“D”产生的事件。

4.12.5　具有服务分发的聚合服务器

图 6 给出了向聚合服务器发送服务请求的客户端，以及通过向底层服务器提交多个服务请求的聚合服务支持的示例。

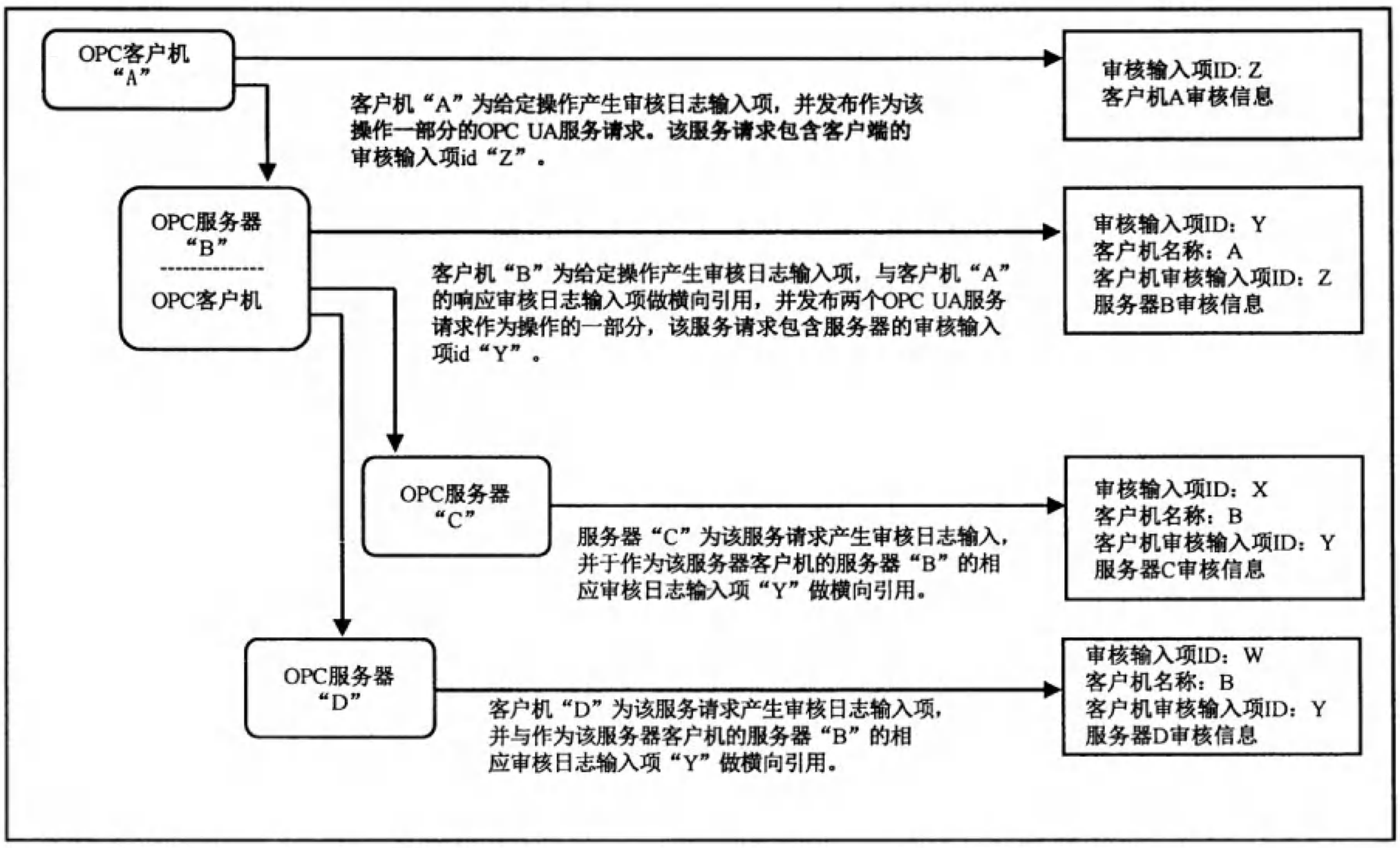

图 6　具有服务分发的聚合服务器

在聚合服务器情况下，也要求服务器向聚合的服务器订阅审核事件。在该模式下，服务器“B”应能向客户端“A”提供所有的审核事件，包括由服务器“C”和服务器“D”产生的事件。

5　安全协调

5.1　针对威胁的 OPC UA 安全机制

5.1.1　概述

后续条处理在 4.3 中描述的针对 OPC UA 功能的威胁。每条都直接与 4.3 中对应条描述的威胁关联。

相比较在 5.2 中给出的目标，本条主要处理与 OPC UA 安全功能相关的特定威胁。

5.1.2　消息洪泛

该威胁的描述见 4.3.2。

OPC UA 通过在消息被鉴别前最小化消息处理的开支，使得消息洪泛造成的可用性损失最小化。这可防止攻击者只用很少的精力却造成合法 OPC UA 应用花费大量时间响应，并占用合法活动的处理资源。

在客户端被识别之前，只有 GetEndpoints（在 IEC 62541-4 中规定）和 OpenSecureChannel（在 IEC 62541-4 中规定）是服务器处理的服务。对 GetEndpoints 的响应仅仅是一组静态信息集，所以服务器不需要做过多处理。对 OpenSecureChannel 的响应需消耗服务器相当多资源，因为需处理签名和加密。OPC UA 已经最小化该处理，但不能去掉该处理。

服务器实现可从两种方式避免 OpenSecureChannel 消息洪泛。

首先，服务器一旦接收到错误 OpenSecureChannel 请求，则可以故意延迟对 OpenSecureChannel 的

处理,以及发出警报提醒工厂工作人员:有攻击,可能屏蔽新的合法的 OpenSecureChannel 请求。

其次,当 OpenSecureChannel 请求次数超过服务器规定的并发最大通道数时,服务器用错误响应作为应答,不进行签名和加密处理。要求已认证的 OPC UA 服务器在其产品文档中规定并发通道的最大数,见 IEC 62541-7。

OPC UA 审核功能向站点提供相关证据,这些证据有助于发现正在进行的洪泛攻击以及找到以后防止此类攻击的方法,(见 4.12)。

OPC UA 依靠站点 CSMS 避免攻击,例如在支持 OPC UA 的协议层和系统的消息洪泛。

5.1.3 窃听

本威胁的描述见 4.3.3。

OPC UA 提供加密避免窃听,见 5.2.4。

5.1.4 消息欺骗

本威胁的描述见 4.3.4。

根据 IEC 62541-4 和 IEC 62541-6 的规定,OPC UA 通过消息签名解决消息欺骗威胁。此外,消息总是包含有效的会话 ID、安全通道 ID、请求 ID 以及正确的序列号。

5.1.5 消息变化

本威胁的描述见 4.3.5。

OPC UA 通过在 IEC 62541-4 中规定的消息签名来应对消息变化。如果消息改变,检查该签名将显示该变化,并允许接收者丢弃该消息。

5.1.6 消息重放

本威胁的描述见 4.3.6。

OPC UA 对于每个请求和响应消息使用会话 ID、安全通道 ID、时间戳、序列号和请求 ID。消息被签名且任何变化都会被侦测,所以重放消息很困难,这样消息应具有有效会话 ID、安全通道 ID、时间戳、序列号和请求 ID。(以上所有内容见 IEC 62541-4 和 IEC 62541-6)。

5.1.7 畸形消息

本威胁的描述见 4.3.7。

OPC UA 客户端和服务器产品实现通过检查消息是否具有正确格式以及消息参数是否在合法范围内,来应对畸形消息威胁。这部分内容见 IEC 62541-4 和 IEC 62541-6。

5.1.8 服务器剖析(Server profiling)

本威胁的描述见 4.3.8。

OPC UA 限制服务器给未经识别的客户端提供的信息量。该信息是 IEC 62541-4 中规定的 GetEndpoints 服务的响应。

5.1.9 会话劫持

本威胁的描述见 4.3.9。

OPC UA 通过为安全上下文(即安全通道)分配在 IEC 62541-4 中 CreateSession 服务规定的会话,来解决会话劫持威胁。劫持会话将首先威胁安全通道。

5.1.10 欺诈服务器

本威胁的描述见 4.3.10。

OPC UA 客户端应用通过验证服务器应用实例证书的有效性，解决欺诈服务器威胁。鉴于欺诈服务器可能提供来自认证 OPC UA 服务器的证书，但它并不拥有合适的用于解密的私有密钥(因为私有密钥绝不会分配)进行解密，并使用合适公共密钥验证保护的消息，所以欺诈服务器决不可能读取和误用客户端发送的安全数据。

5.1.11 用户凭证泄密

本威胁的描述见 4.3.11。

OPC UA 通过 5.2.4 中描述的加密，保护在网上发送的用户凭证。OPC UA 依靠站点 CSMS，防止想获取用户凭证的其他攻击，如猜测密码或社会工程。

5.2 面向实现目标的 OPC UA 安全机制

5.2.1 概述

以下内容使用 OPC UA 功能实现 4.2 中描述的目标。后续内容与 4.2 中对应条的目标直接相关。

相比 5.1 中处理威胁，本条证实 OPC UA 安全结构的完备性。

5.2.2 鉴别

5.2.2.1 概述

OPC UA 应用支持正在通信实体的鉴别，以及向其他实体提供必要鉴别凭证。

5.2.2.2 应用鉴别

根据 IEC 62541-4 中的 GetEndpoints 和 OpenSecureChannel 服务规定，OPC UA 客户端和服务器应用通过 http://tools.ietf.org/html/rfc3174 X.509 证书 (见[X509])[1)] 各自进行识别并鉴别。一些通信栈要求这些证书代表主机或用户，而不是应用。

5.2.2.3 用户鉴别

根据 IEC 62541-4 中 OpenSecureChannel 的服务的描述，OPC UA 客户端接收来自用户的用户标识令牌，并将令牌传递给 OPC UA 服务器。OPC UA 服务器鉴别该用户令牌。OPC UA 应用接收如下三种格式令牌的其中一种：用户名/密码，X.509v3 证书 (见[X509])，或 WS-SecurityToken。

根据 IEC 62541-4 中 CreateSession 和 ActivateSession 服务部分的规定，如果用户标识令牌是数字证书，则该令牌使用挑战-响应(challenge-response)过程进行验证。服务器提供 Nonce 和签名算法作为在 CreateSession 响应的挑战。客户端通过签名服务器的 Nonce 并将其作为后续 ActivateSession 调用中的参数，来响应该挑战。

5.2.3 授权

OPC UA 未规定如何提供用户或客户端授权。作为大型工业自动化产品一部分的 OPC UA 应用，可以通过该产品的授权管理来管理授权一致性。为确定用户授权，用户的标识和授权在 OPC UA 中规定，因此客户端和服务器应用能识别该用户。

---

1) 见参考文献。

OPC UA 服务器使用 Bad_UserAccessDenied 错误码作为响应，按 IEC 62541-4 中的状态代码部分指示授权或授权错误。

5.2.4 机密性

OPC UA 使用对称和非对称加密保护作为安全目标的机密性。因此非对称加密用于密钥约定，对称加密用于保护 OPC UA 应用间发送的所有其他消息。加密机制的规定见 IEC 62541-6。

OPC UA 依靠站点 CSMS 保护在网络和系统架构的机密性。OPC UA 依靠 PKI 管理用于对称和非对称加密的密钥。

5.2.5 完整性

OPC UA 使用对称和非对称签名实现作为安全目标之一的完整性。非对称签名用于建立安全通道过程中的密钥约定阶段。对称签名适用于所有其他消息。

OPC UA 依靠站点 CSMS 保护网络和系统架构的完整性。OPC UA 依靠 PKI 管理用于对称和非对称签名的密钥。

5.2.6 可审核性(Auditability)

根据 IEC 62541-4 中 UA 审核部分的规定，OPC UA 通过提供活动的可追溯性来支持审核日志，活动的可追溯性通过多个发起、转发和处理活动的客户端和服务器的活动日志输入项保证。OPC UA 依靠 OPC UA 应用产品提供有效的审核日志方案或有效的收集所有节点审核事件的模式。该方案可能是 OPC UA 应用所在的大型工业自动化产品的一部分。

5.2.7 可用性

OPC UA 最小化消息洪泛的影响，见 5.1.2。

对可见性的攻击包括打开超过服务器能处理的更多会话，由此可导致服务器失效或运行困难。服务器拒绝超过规定的最大数量的会话。

6 实现考虑

6.1 概述

本章为实现 OPC UA 应用的制造商提供指导。鉴于解决上述威胁所必需的许多对策超出了 OPC UA 规范的范围，因此本章给出如何提供这些对策的建议。

对后续内容，本章定义了问题范围、识别未采取合适对策而产生的后果，以及推荐最好的实现方法。

6.2 适当的超时

超时，实现必须等待的时间(通常等待某个事件，例如：消息到达)，在影响实现安全性方面发挥重要作用。潜在结果包括：

——拒绝服务：如果超时很大，当客户端未重启会话时可能会存在拒绝服务的条件；

——资源消耗：当客户端长时间处于空闲状态时，服务器应保留该时间段的客户端信息，这会导致资源耗尽。

对于每个连接阶段实施者宜使用合理的超时。

6.3 严格消息处理

本标准规定正确消息的格式，但未规定实现如何处理不符合规范的消息。通常实现继续解析这些

包,这将导致脆弱性。

——实现应对消息格式进行严格地检查,如格式错误则应丢弃包或发送错误消息。

——错误处理使用最适合该条件的错误码,见 IEC 62541-4。

6.4 随机数生成

满足安全需要的随机数可由密码库提供的适当函数产生。由 CRT 提供的通用随机数函数,如使用 rand()方法,不能产生足够的熵。实现者可以替代使用 MS windows 密码库(WinCrypt 库)或由 OpenSSL 提供的随机数发生器。

6.5 特定和保留数据包

实现必须理解并正确解释保留作为特定(例如在 IP 规范中广播地址和组播地址)的任何消息类型。不能理解和解释这些特定数据包可能导致脆弱性。

6.6 速率限制和流量控制

OPC UA 不提供速率控制机制,但实现能增加速率控制。

参 考 文 献

[1] SOAP Part 1: SOAP Version 1.2 Part 1: Messaging Framework, available at <http://www.w3.org/TR/ soap12-part1/>

[2] SOAP Part 2: SOAP Version 1.2 Part 2: Adjuncts, available at <http://www.w3.org/TR/soap12-part2/>

[3] XML Encryption: XML Encryption Syntax and Processing, available at <http://www.w3.org/TR/xmlenc -core/>

[4] XML Signature:: XML-Signature Syntax and Processing, available at <http://www.w3.org/TR/xmldsig -core/>

[5] WS Security: SOAP Message Security 1.1, available at<http://www.oasis-open.org/committees/ download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>

[6] WS Addressing: Web Services Addressing (WS-Addressing), available at <http://www.w3.org/ Submission/ws-addressing/>

[7] WS Trust: Web Services Trust Language (WS-Trust), available at <http://specs.xmlsoap.org/ws/ 2005/02/trust/WS-Trust.pdf>

[8] WS Secure Conversation: WebServices Secure Conversation Language (WSSecureConversation),available at <http://specs.xmlsoap.org/ws/2005/02/sc/WS-SecureConversation.pdf>

[9] SSL/TLS: RFC 2246: The TLS Protocol Version 1.0, available at <http://www.ietf.org/rfc/rfc2246.txt>

[10] :X509: X.509 Public Key Certificate Infrastructure, available at <http://www.itu.int/rec/T-REC-X.509 —200508-I/en>

[11] HTTP: RFC 2616: Hypertext Transfer Protocol - HTTP/1.1, available at <http://www.ietf.org/rfc/ rfc2616.txt>

[12] HTTPS: RFC 2818: HTTP Over TLS, available at <http://www.ietf.org/rfc/rfc2818.txt>

[13] IS Glossary: Internet Security Glossary, available at <http://www.ietf.org/rfc/rfc2828.txt>

[14] NIST 800-12: Introduction to Computer Security, available at <http://csrc.nist.gov/publications/ nistpubs/800-12/>

[15] NERC CIP: CIP 002-1 through CIP 009-1, by North-American Electric Reliability Council,available at <http://www.nerc.com/docs/standards/sar/Cyber_Security_Standards_Board_Approval 2May06.pdf>

[16] IEC 62351: Data and Communications Security, available at <http://webstore.iec.ch/webstore/ webstore.nsf/mysearchajax? Openform&key=62351>

[17] SPP-ICS: System Protection Profile—Industrial Control System, by Process Control Security

[18] Requirements Forum (PCSRF), available at <http://www.isd.mel.nist.gov/projects/processcontrol /SPP-ICSv1.0.pdf>

[19] SHA-1: Secure Hash Algorithm RFC, available at <http://tools.ietf.org/html/

rfc3174>

[20] PKI: Public Key Infrastructure article in Wikipedia, available at <http://en.wikipedia.org/wiki/Public_ key_infrastructure>

[21] X509 PKI: Internet X.509 Public Key Infrastructure, available at http://www.ietf.org/rfc/rfc3280.txt>

中 华 人 民 共 和 国
国 家 标 准
OPC 统一架构 第 2 部分:安全模型
GB/T 33863.2—2017/IEC/TR 62541-2:2010
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 46 千字
2017 年 7 月第一版 2017 年 7 月第一次印刷
*
书号:155066·1-56668 定价 27.00 元

GB/T 33863.2-2017