文章编号:2095-476X(2012)06-0105-04

工业网络中非标准 VPN 的安全技术研究

朱鹏, 张智斌, 黄昱泽

(昆明理工大学 信息工程与自动化学院, 云南 昆明 650500)

摘要:针对在工业控制领域中,传统的监控与数据采集独立运转且很少配置安全管理的问题,利用N2N为工业网络之间的通信构建一条安全通道,使用数字证书对加入的节点进行身份验证,借助IKEv2协议实现节点之间的协商通信,并通过动态选择加密算法及通信密钥,有效提高了N2N在工业网络通信中的安全性.

关键词:N2N;监控与数据采集;工业网络通信

中图分类号:TP393.08 **文献标志码**:A DOI:10.3969/j.issn.2095-476X.2012.06.028

Study on non-standard VPN security technology in the industrial network

ZHU Peng, ZHANG Zhi-bin, HUANG Yu-ze

(*Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming* 650500, *China*)

Abstract: Aiming at the problem that the traditional SCADA (supervision control and data acquisition) is operated independently with less configuration safety management in current industrial control field, a secure channel was constructed the communication between industrial network using N2N (a layer two peer-to-peer VPN), in which the joining node will be authenticated with digital certificates, and node communication between joint be realized with IKEv2 protocol. As a result, the security of N2N in industrial network communication will be improved efficiently and greatly through dynamic selective encryption algorithm and communication key.

Key words: a layer two peer-to-peer VPN; supervision control and data acquisition; industrial network communication

0 引言

目前,监控与数据采集SCADA(supervision control and data acquisition)系统在工业控制领域中应用广泛,很多工程人员通过其对工业设备进行实时监控管理.随着互联网的普及,工业自动化控制技术的应用从局部范围扩大到整个网络世界,在某些领域的需求越来越强烈.由于传统的工业网络不提供安全管理机制,直接将工业网络与Internet相连,容易受到非法用户的入侵,数据在传输的过程中易被窃取.而对于SCADA系统来说,系统中的很多设备不能安装相关安全客户端软件,为了保证工业网络中的数据安全,可在各个SCADA系统中配置一台N2N(a layer two peer-to-peer VPN)客户端机器,通过对N2N客户端进行功能扩充,使之能收集需要发送到其他SCADA系统的数据,并将其加密后传输;也能够接收其他SCADA系统传来的数据,并将其解密后分发给系统中的工业设备.通过使用N2N

收稿日期:2012-07-05

作者简介:朱鹏(1987—),男,湖南省双峰县人,昆明理工大学硕士研究生,主要研究方向为计算机网络.

在 Internet 上构建安全通道,来保证数据在 Internet 上的安全传输,实现 SCADA 系统从区域到全域的管理. 本文主要对应用工业网络互联的 N2N 安全技术进行研究,通过将 PKI 技术和 IKEv2 协议引入其中,增强 N2N 的安全性,进而保证使用 N2N 进行互联的工业网络的安全性.

1 N2N 在工业网络中的安全问题分析

N2N 是一个通用型的 P2P-VPN 程序[1],使用预共享密钥管理方式,只提供 Twofish 加密算法. 如果将 N2N 直接用来实现工业网络互联,可能会产生较大的安全隐患. 本文主要从认证管理、密钥管理和加解密算法 3 个可待加强的方面进行分析.

1)认证管理. N2N 允许用户自行创建 super node 端和 edge 端,edge 端注册过程如下:用户在启动 edge 端以后向已启动的 super node 端发送注册信息,super node 在收到注册信息以后,就在注册链表中查询该 edge 是否注册,如果没有注册,super node 就将 edge 加入到注册链表中,完成注册. 而对于 SCADA 系统来说,如果 super node 不对 edge 进行严格的身份认证,允许任意 edge 加入网络,这可能会给系统带来毁坏性的破坏. 因此对于用于工业网络互联的 N2N 来说,需要在 edge 注册之初对 edge 进行严格的身份认证,只允许合法用户加入到网络中,从而避免非法用户入侵网络.

2)密钥管理. N2N 中用来加密解密的密钥使用预共享的方式,数据的加密解密都在 edge 端进行. 在启动 edge 时,可以选择手工输入密钥或者从已配置好的密钥文件中读取密钥,只有 edge 双方都使用相同的密钥时,数据信息才能被解密. 然而对于工业网络来说,为了保持网络的稳定性,保障各个网络之间信息的互通性,整个网络长时间使用预共享密钥对数据进行加密解密,会给工业网络带来巨大的风险以及管理上的困难.

3)加密解密算法. 在 N2N 的源程序中,只使用了一个 Twofish 加密算法对数据进行加密解密,虽然 Twofish 的抗差分攻击能力以及抗相关密钥 Slide 攻击的能力都很强,但由于工业网络的特殊性以及被破坏所带来的毁坏性,可在程序中部署多种成熟的加密算法供动态选择,将增强数据的安全性,从而更好地为工业网络保驾护航.

2 N2N 在工业网络中安全技术的设计

对于直接将 N2N 应用于工业网络存在的安全问题,可以使用 edge 向 super node 注册之前进行身份认证、edge 之间通信之前进行密钥协商以及选择加密算法的方式进行解决. 而身份认证与密钥协商都是在注册成功之前或数据发送之前进行的,将认证和协商与通信分离,能更好地为数据提供安全保护.

在各种不同的身份认证机制中,基于数字证书的身份认证是最灵活和安全的. super node 与 edge 之间的身份认证可以结合 PKI 技术来完成,所有需要进入网络的用户设备都需要有确定的身份证书. 在这里,主要是借助认证中心(CA)来为用户提供安全保证. CA 为每个用户或设备发放一张身份数字证书,利用 CA 强大的管理功能,证书的发放、维护和撤销等管理就比较容易. 而由于数字证书具有唯一性,对于移动用户也可以很方便地进行身份认证.

在 N2N 中,数据信息的加密过程都是在 edge 中完成的,当某个 edge 需要和其他 edge 进行数据通信时,该 edge 先与接收信息的 edge 就通信过程中所用的加密算法、通信 SA(security association)进行协商,只有当双方协商成功之后,双方的数据通信才能进行. 改进后的 N2N 安全设计总体框架图如图 1 所示.

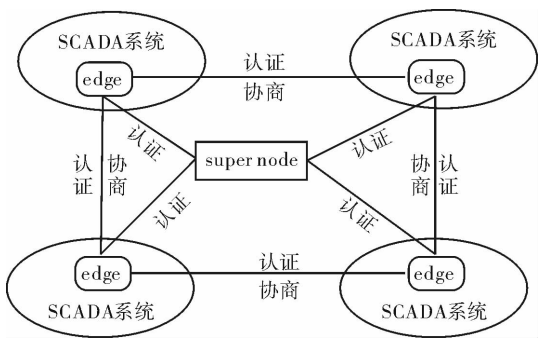

图 1 安全设计总体框架图

2.1 edge 与 super node 数字签名的认证过程

认证结构的 PKI 环境[2]主要由认证中心 CA、注册中心 RA 和 LDAP 服务器组成. CA 是签发和管理证书的实体;RA 负责核查申请证书实体的身份,并完成提交数据正确性验证;LDAP 用来存储签发的属性证书和属性证书撤销列表. 整个系统的认证

模型如图 2 所示.

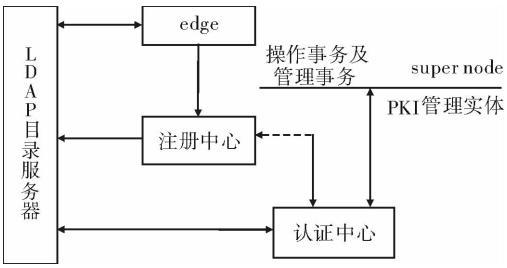

图 2　系统认证模型

edge 认证过程[3]如下:

1)edge E 发起认证请求,将自己的身份、认证信息 AUTH 以及随机数 nonce 发送给 super node S;

2)S 收到 E 发来的验证请求后,对 E 的身份进行验证,验证通过则向 E 发送自己的身份、认证信息 AUTH 以及随机数 nonce;

3)E 验证 S 身份后,向 S 发送注册请求;

4)S 收到 E 的注册请求后,返回一个注册成功数据包.

在整个注册认证过程中,如果 edge 端没有申请数字证书,则向 RA 发送一个证书请求,RA 审核后提交证书请求给认证机构 CA. CA 对证书申请请求进行处理,签署并颁发用户证书,并且登记在证书库中,同时定期更新证书失效列表,供用户查询. edge 在收到 CA 颁发的证书后,将证书封装在注册包中,一起发送给 super node. super node 收到 edge 发来的注册信息,解析注册信息并对其中的数字证书进行验证,如果证书有效,则通过身份认证,完成注册,如认证不通过,终止注册.

2.2　edge 与 edge 通信协商的实现

在 N2N 的源程序中,只要 edge 注册到 super node 以后,就可以向其他 edge 发送信息,若目的 edge 不在发送 edge 的认证链表中,则把信息转发给 super node. super node 在接收到信息后,根据目的 edge 的 MAC 地址在其注册链表中进行查询,如果目的 edge 存在于注册链表中,则向该 edge 转发信息,否则丢弃该信息. 目的 edge 在收到 super node 转发过来的信息后,如果解析到 edge 不在认证链表中,则向该发送 edge 发送一个认证包,发送 edge 在收到目的 edge 发来的认证包后,返回给目的 edge 一个确认认证包,完成认证.

改进后的认证模式是在原有认证过程前加入一个协商过程,使得 edge 与 edge 在进行通信之前,必须对对方的身份、通信的加密算法以及密钥进行协商;通信过程将使用协商的加密解密算法和密钥进行通信. 在协商过程中,主要借助 IKEv2 协议加以实现[4], IKEv2 的协商过程如图 3 所示.

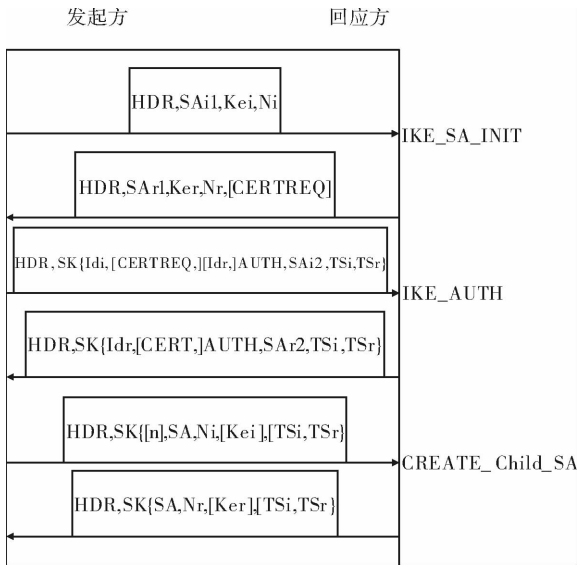

图 3　IKEv2 协商过程

结合 IKEv2 的 edge 与 edge 之间的通信协商[5]过程如下:

1)edge A 发起连接请求,向 edge B 发送安全关联的 SA 提议、DH 交换的临时公共值 KEa 和防重放攻击的随机数 Na.

2)B 在收到 A 的连接请求后,从 A 的提议中选择一个提议,并将自己用于 DH 交换的临时公共值 KEb、防重放攻击的随机数 Nb 以及查询 A 的证书请求返回给 A.

3)A 收到 B 的回应后,向 B 发送用于 N2N 加密的 SA 提议以及自己的身份信息、证明、对方的身份信息请求和流量选择符.

4)B 对 A 的身份进行认证,通过后选择一个 SA 提议,将自己的身份信息 ID,认证载荷 AUTH 及流量选择符返回给 A,完成初始化交互.

5)A 在对 B 进行身份验证后,向 B 发送 SA 提案,交换 nonce、流量选择符 TSi 和 TSr 以及可选的进行 DH 交换值 Kei,发送信息使用前一次通信协商的加密算法和 B 的公钥进行加密.

6)B 在收到 A 的信息后,使用私钥进行解密,并对 A 的 SA 提案和流量选择符进行响应,交换 nonce.

整个协商过程由 6 条消息组成[6]. 其中 1)和 2)两条消息用来协商密码算法、交换 nonce 和 DH 公共值;3)和 4)两条消息用来对前面的消息进行认证和交换各自的身份,并建立第 1 个 Child_SA;5)和6)可由通信的任一方在前 4 条消息交换结束后发起,以生成额外的 Child_SA 或重新进行密钥协商(rekeying).

当 edge A 与 edge B 在前4 条信息交换成功后,就可以选择第 5,6 条消息中生成的 Child_SA 进行通信了. 在通信过程中根据协商好的 Child_SA 选择加密算法,使用计算出的密钥对数据进行加密. 在这个解决方案里,可供 SA 进行协商的密码库采用的是 OpenSSL 提供的密钥算法库. 在整个协商过程中,edge 可以自动选择加密算法,通过创建 Child_SA 来确保在通信过程中实现加密算法及密钥的动态切换,从而避免预共享密钥管理方式以及加密算法单一的安全隐患,更好地保证数据在传输过程中的安全性.

3 结论

本文对应用于工业网络互联的非标准 VPN 的安全技术进行了研究,通过使用数字证书认证,使得 edge 只有在通过 super node 身份认证后才能完成注册,而在 edge 与 edge 通信前使用 IKEv2 协议进行协商,动态选择加密算法及通信密钥,增强 N2N 在工业网络通信过程中的安全性. 然而工业网络是一个非常复杂的网络,它的涉及面非常广,对安全性的要求非常高,因此还有许多问题有待进一步的研究.

参考文献:

[1] Deri L, Andrews R. N2N: A layer two peer-to-peer VPN [J]. LNCS, 2008, 5127: 53 - 64.

[2] 张小波,程良伦. PKI 在虚拟专用网络中的应用[J]. 计算机工程,2011,37(15):113.

[3] 寇晓蕤,王清闲. 网络安全协议——原理、结构与应用[M]. 北京:高等教育出版社,2009.

[4] 邱司川,潘进,刘丽明. IKEv2 协议的分析与改进[J]. 计算机工程,2009,35(15):126.

[5] 韩旭东,汤隽,郭玉东. 新一代 IPSec 密钥交换规范 IKEv2 的研究[J]. 计算机工程与设计,2007,28(11):2549.

[6] 韩明奎,潘进,李波. 一种改进的 IKEv2 协议及其形式化验证[J]. 计算机应用研究,2010,27(2):707.