ICS 29.240.30
F 21

中华人民共和国国家标准化指导性技术文件

GB/Z 25320.3—2010/IEC TS 62351-3:2007

电力系统管理及其信息交换 数据和通信安全 第3部分:通信网络和系统安全 包括TCP/IP的协议集

Power systems management and associated information exchange—Data and communications security—Part 3:Communication network and system security—Profiles including TCP/IP

(IEC TS 62351-3:2007,IDT)

2010-11-10 发布　　2011-05-01 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

国际电工委员会57技术委员会(IEC TC 57)对电力系统管理及其信息交换制定了IEC 62351《电力系统管理及其信息交换　数据和通信安全》标准。我们采用IEC 62351，编制了GB/Z 25320指导性技术文件，主要包括以下部分：

——第1部分：通信网络和系统安全　安全问题介绍；

——第2部分：术语；

——第3部分：通信网络和系统安全　包含TCP/IP的协议集；

——第4部分：包含MMS的协议集；

——第5部分：IEC 60870-5及其衍生标准的安全；

——第6部分：DL/T 860的安全；

——第7部分：网络和系统管理的数据对象模型；

——第8部分：电力系统管理的基于角色访问控制。

本部分等同采用IEC TS 62351-3:2007《电力系统管理及其信息交换　数据和通信安全　第3部分：通信网络和系统安全　包含TCP/IP的协议集》(英文版)。

本部分由中国电力企业联合会提出。

本部分由全国电力系统管理及其信息交换标准化技术委员会(SAC/TC 82)归口。

本部分起草单位：辽宁省电力有限公司调度通信中心、国网电力科学研究院、国家电力调度通信中心、中国电力科学研究院电网自动化研究所、福建省电力有限公司电力调度通信中心、华中电网有限公司电力调度通信中心、华东电网有限公司。

本部分主要起草人：曹连军、南贵林、许慕樑、韩水保、杨秋恒、邓兆云、李根蔚、袁和林、林为民。

本指导性技术文件仅供参考。有关对本指导性技术文件的建议或意见，向国务院标准化行政主管部门反映。

引　言

计算机、通信和网络技术当前已在电力系统中广泛使用。通信和计算机网络中存在着各种对信息安全可能的攻击，对电力系统的数据及通信安全也构成了威胁。这些潜在的可能的攻击针对着电力系统使用的各层通信协议中的安全漏洞及电力系统信息基础设施的安全管理的不完善处。

为此，我们采用国际标准制定了GB/Z 25320《电力系统管理及其信息交换　数据和通信安全》，通过在相关的通信协议及在信息基础设施管理中增加特定的安全措施，提高和增强电力系统的数据及通信的安全。

电力系统管理及其信息交换 数据和通信安全 第3部分:通信网络和系统安全 包括TCP/IP的协议集

1 范围和目的

1.1 范围

GB/Z 25320的本部分规定如何为SCADA和用TCP/IP作为消息传输层的远动协议,提供机密性、篡改检测和消息层面认证。

虽然对TCP/IP的安全防护存在许多可能的解决方案,但本部分的特定范围是在端通信实体内TCP/IP连接的任一端处,提供通信实体之间的安全。对插入其间的外接安全装置(如"链路端加密盒")的使用和规范不在本部分范围内。

1.2 目的

GB/Z 25320的本部分规定如何通过限于传输层安全协议(Transport Layer Security,TLS)(在RFC 2246中定义)的消息、过程和算法的规范,对基于TCP/IP的协议进行安全防护,使这些协议能适用于IEC TC 57的远动环境。如其他IEC TC 57标准需要为它们的基于TCP/IP协议提供防护,则本部分预期作为这些IEC TC 57标准的规范性部分而被引用。然而,决定是否引用本文件是各个协议安全防护的自主选择。

本部分反映了目前IEC TC 57协议的安全需求。如果其他标准将来提出新的需求,本部分也许需要修订。

本部分的初期读者预期是在IEC TC 57中制定或使用这些协议的工作组成员。为使本部分描述的措施有效,对于使用TCP/IP的协议本身,其规范就应采纳和引用这些措施。本部分就是为了使得能这样处理而编写的。

本部分的后续读者预期是实现这些协议的产品的开发人员。本部分的某些部分也可以被管理人员和执行人员使用,以理解该工作的目的和需求。

2 规范性引用文件

下列文件中的条款通过GB/Z 25320的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/Z 25320.1 电力系统管理及其信息交换 数据和通信安全 第1部分:通信网络和系统安全安全问题介绍(GB/Z 25320.1—2010,IEC TS 62351-1:2007,IDT)

IEC TS 62351-2 电力系统管理及其信息交换 数据与通信安全 第2部分:术语(Power systems management and associated information exchange—Data and communications security—Part 2:Glossary of terms)

RFC 2246 传输层安全协议(TLS)(RFC 2246:1999,The TLS Protocol Version 1.0[1])

1) T. Dierks,C. Allen。通常该标准称为SSL/TLS(安全套接层/传输层安全协议)。

RFC 2712 外加于 TLS 的 Kerberos 密码套件[RFC 2712:1999, Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)[2)]]

RFC 3268 TLS 的高级加密标准(AES)密码套件[RFC 3268, 2002, Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)]

RFC 3280 因特网 X.509 PKI 证书和证书撤销列表(CRL)格式[RFC 3280, 2002, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile]

3 术语和定义

IEC 62351-2 中给出的术语和定义适用于 GB/Z 25320 的本部分。

4 本部分涉及的安全问题

4.1 在远动环境中影响使用 TLS 的运行要求

与许多为提供安全防护而采用 TLS 的信息技术(IT)协议相比,IEC TC 57 的远动环境具有不同运行需求。就安全防护来说,最大的差异在于 TCP/IP 连接的持续时间,在此持续时间内需要为该连接维持安全防护。

许多 IT 协议连接的持续时间很短,这使加密算法能在连接重新建立时再协商。然而,远动环境中连接趋向于更长的持续时间,而且经常是"永久的"。正是 IEC TC 57 连接的长久性产生了特殊考虑的需要。关于这点,为了提供"永久"连接的机密性,本部分规定了加密密钥再协商的透明机制。

本部分解决的另一个问题是如何达到不同实现之间的互操作性。TLS 允许在建立连接时支持和协商各种密码套件。因而可以料想,两个实现可能各自会支持互斥的密码套件集合。所以本部分规定涉及标准必须指定至少一套允许互操作的公共密码套件和一组 TLS 参数。

此外,本部分还规定了使用特殊 TLS 能力,使得能应对特定的安全威胁。

4.2 应对的安全威胁

安全威胁和攻击方法的讨论,详见 GB/Z 25320.1。

TCP/IP 和本部分中的安全规范仅针对通信的传输层(OSI 第 4 层及以下)。本部分并不包括通信的应用层(OSI 第 5 层及以上)的安全或应用对应用的安全。

对该传输层,本部分要应对的特定威胁包括:

- 通过消息层面认证和消息加密,应对未经授权访问信息;
- 通过消息层面认证和消息加密,应对未经授权修改(即篡改)或窃取信息。

4.3 应对攻击的方法

通过本部分中规范和建议的适当实现,应对以下安全攻击的方法:

- 中间人:通过使用本部分中指定的消息鉴别码机制来应对该威胁;
- 重放:通过使用在 RFC 2246,RFC 2712 和 RFC 3268 中规定的专用处理状态机来应对该威胁;
- 窃听:通过使用加密来应对该威胁。

注:对于声称符合本部分的实现,其实际性能特性不在本部分的范围之内。

5 强制要求

5.1 严禁使用不加密的密码套件

不应使用任何规定加密为 NULL 的密码套件。

禁用的密码套件列表如下,但不限于这些:

TLS_NULL_WITH_NULL_NULL;

2) A. Medvinsky, M. Hur..

TLS_RSA_WITH_NULL_NULL_MD5;

TLS_RSA_NULL_WITH_NULL_SHA。

5.2 版本协商

只有对应于安全套接层 3.1 版以上(SSL 3.1 或更高版本)的 TLS 1.0 是允许的。早于 SSL 3.1 的版本将导致无法建立连接。

5.3 密码再协商

声称符合本部分的实现应明确说明对称密钥将基于一个时间周期和最大允许发送分组数或字节数进行再协商。对引用本部分的标准,该引用标准的 PIXIT(Protocol Implementation eXtra Information for Testing,协议实现的测试附加信息)应给出对再协商限制的规定。

再协商值应是可配置的。

发起变更密码序列应是接收到 TCP-OPEN 指示原语的 TCP 实体(即被叫实体)的责任,而从主叫实体(即发出 TCP-OPEN 原语的节点)所发出的变更密码请求应不予理会。

应有一个与变更密码请求的响应相关的超时机制。变更密码请求超时应导致连接被终止。超时值应是可配置的。

5.4 消息鉴别码

应使用消息鉴别码。

注:TLS 具有使用消息鉴别码的能力,规定作为选项。本部分要求使用消息鉴别码,以有助于应对和检测中间人攻击。

5.5 证书支持

5.5.1 多证书机构(CA)

声称符合本部分的实现应支持一个以上的证书机构(Certificate Authority,CA)。实际数目应在实现的 PIXIT 声明中说明。

证书机构(CA)的标准和选择不是本部分的范围。

5.5.2 证书长度

确定使用本部分的协议应规定允许使用的证书最大长度。建议该长度不大于 8 192 个字节。

5.5.3 证书交换

证书的交换和确认应是双向的。如果任一方实体不提供证书,连接应被终止。

5.5.4 证书比对

证书应由主叫节点和被叫节点双方确认。证书验证有两种机制,机制应是可配置的:

- 接受出自授权的证书机构(CA)的任何证书;
- 接受出自授权的证书机构(CA)的个体证书。

5.5.4.1 基于证书机构(CA)的验证

声称符合本部分的实现应可配置为接受出自一个或多个证书机构的证书而不必配置个体证书。

5.5.4.2 基于个体证书的验证

声称符合本部分的实现应可以被配置为接受出自一个或多个授权的证书机构(例如已设定的证书机构)的特定个体证书。

5.5.4.3 证书撤销

应按 RFC 3280 的规定执行证书撤销。

证书撤销列表(CRL)的管理是一个当地实现的问题。关于 CRL 管理问题的讨论能够在 GB/Z 25320.1 中找到。

声称符合本部分的实现应有能力以可配置的时间间隔对当地 CRL 进行检查。检查 CRL 的过程不应导致已建立的连接终止。不能访问 CRL 不应导致连接终止。

在建立连接时不应使用已撤销证书。在连接建立期间接收到已撤销证书的实体应拒绝本次连接。

证书撤销应终止使用该证书所建立的任何连接。

引用本部分的其他标准应指定推荐的缺省评估时间间隔。如果当前正使用的证书已被撤销，该引用标准应决定将要采取的行动。

注：通过 CRL 的正常应用或发布，连接就可能被终止而造成无法进行通信。因而系统管理员应当规定证书管理过程，以减少此类事件的发生。

5.5.4.4 过期证书

证书到期不应导致连接终止。

在连接建立期间过期证书不应使用或接受。

5.5.4.5 签名

应支持使用 RSA 和 DSS 算法进行签名。在引用本部分的标准中可指定其他算法。

5.5.4.6 密钥交换

密钥交换算法应支持密钥的最大长度至少为 1 024 比特。应支持 RSA 和 Diffe-Hellman 两种机制。

5.6 与非安全协议通信流共存

各引用标准都应提供一个单独的 TCP/IP 端口，通过此端口交换经 TLS 防护的通信流。这将是考虑到完全明确的安全和非安全通信同时进行的可能性。

6 TC 57 引用标准的要求

引用本部分的其他标准应规定：

- 所支持的强制密码套件；
- 推荐的交换加密密钥时间周期；
- 关于基于协议通信流的密钥再协商的建议规范。这将规定用于度量该通信流的机制(例如，已发送分组数，已发送字节数等)和宜执行再协商的建议标准；
- 所支持的证书机构(CA)的建议数量；
- 为了区分安全(例如使用 TLS)通信流和非安全通信流所使用的 TCP 端口；
- 最大证书长度；
- 宜规定建议的缺省 CRL 评估周期；
- 对本部分所要求的一致性。

7 一致性

实现第 5 章的所有要求将决定符合于本部分的一致性。